Załącznik nr 1 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

wraz ze wskazaniem wymagań technicznych , użytkowych i jakościowych

odnoszących się do głównych elementów składających się na przedmiot zamówienia

**NAZWA ZAMÓWIENIA:**

**Dostawa sprzętu informatycznego oraz oprogramowania**

**Część 1 Zamówienia :** Dostawa macierzy

**Część 2 Zamówienia :** Dostawa serwera do wirtualizacji wraz z systemem operacyjnym

**Część 3 Zamówienia :** Dostawa systemu NAC

**ZAMAWIAJĄCY :**

Gmina Świętochłowice

ul. Katowicka 54

41-600 Świętochłowice

**Część 1 Zamówienia :** Dostawa macierzy

**1.1 Dostawa macierzy dyskowej – 1kpl**

|  |  |
| --- | --- |
| Wymagania techniczne i użytkowe | |
| Obudowa | Obudowa o wysokości maksymalnie 2U dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie. Co najmniej 24 zatoki przystosowane do instalacji dysków NVMe. |
| Kontroler dyskowy | Zainstalowane minimum dwa redundantne kontrolery pamięci dyskowej, pracujące w trybie symetrycznym Active-Active, obsługujące protokół komunikacji NVMe z dyskami. Pod określeniem tryb Active-Active Symetryczny Zamawiający rozumie, że zasób pamięci dyskowej jest równolegle dostępny na co najmniej 4 portach należących do co najmniej 2 różnych kontrolerów pamięci dyskowej. Każdy z kontrolerów musi mieć możliwość prezentacji wszystkich wolumenów utworzonych w ramach całej pamięci dyskowej. Dodatkowo kontrolery musza posiadać wbudowaną funkcjonalność szyfrowania dysków w standardzie AES 256. |
| Procesor | Architektura przetwarzania danych w ramach procesów wewnętrznych na kontrolerach musi być realizowana za pomocą procesorów firmy Intel serii co najmniej Sapphire Rapids.  Każdy z kontrolerów musi być wyposażony w procesor 12C każdy o taktowaniu minimum 2.1GHz |
| Rozbudowa przestrzeni | Dostarczone rozwiązanie musi umożliwiać podłączenie posiadanych przez zamawiającego innych macierzy dyskowych i przedstawienie ich jako kolejnych pul dyskowych, które można uwzględniać w automatycznych politykach migrowania danych.  Rozwiązanie musi umożliwiać podłączenie minimalnie do 64PiB przestrzeni zewnętrznych, połączenie to musi być realizowanie niezależnie od typu infrastruktury sieciowej sieci SAN (FC lub iSCSI).  Do realizacji powyższej funkcjonalności dostarczone rozwiązanie musi wykorzystywać swoje kontrolery, niedopuszczalne jest stosowanie rozwiązań zewnętrznych, tak zwanych wirtualizatorów.  Licencja na powyższą funkcjonalność nie jest częścią bieżącego postępowania. |
| Zasilacz | Dwa w pełni redundantne zasilane prądem 230V |
| Porty sieciowe | Każdy z dostarczanych kontrolerów pamięci dyskowej musi być wyposażony w co najmniej 4 interfejsy iSCSI, każdy o przepustowości co najmniej 25 Gbps. Porty powinny zapewniać również komunikację z prędkością 10 Gbps. Każdy z Portów musi być obsadzony właściwą do komunikacji wkładką. |
| Dyski | Co najmniej 15 wewnętrznych dysków, każdy w technologii co najmniej NVMe 1.4, każdy o pojemności co najmniej 3.8 TB i posiadający podwójne interfejsy do komunikacji z kontrolerami pamięci dyskowej. |
| Dodatkowe półki dyskowe | Macierz musi posiadać możliwość rozbudowy do minimum 72 dysków NVMe. |
| Gwarancja | * Co najmniej 3 lata gwarancji producenta. * Uszkodzone dyski pozostają własnością Zamawiającego. * Macierz musi być fabrycznie nowa , wyprodukowana nie wcześniej niż 12 miesięcy przed dostawą i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta należy załączyć do oferty |
| Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu **(**odpowiedni dokument należy załączyć do oferty ). * Deklaracja zgodności CE dla urządzenia ( odpowiedni dokument należy załączyć do oferty ). * Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy) |
| **Parametry szczegółowe** | |
| Pełna wewnętrzna redundancja kontrolerów, portów wewnętrznych, zasilania, chłodzenia i ścieżek danych na poziomie minimum N+1.Możliwość uaktualniania oprogramowania systemowego bez przerywania działania pamięci dyskowej, z utrzymaniem wszystkich funkcjonalności oraz z równoczesnym utrzymaniem dostępu do danych poprzez wszystkie ścieżki komunikacyjne Front-End z obydwu kontrolerów.Macierz dyskowa musi być wyposażona w system zapewniający bezpieczne, bez utraty danych, automatyczne wyłączenie w przypadku całkowitego zaniku zasilania.W przypadku awarii zasilania dane z pamięci cache muszą być zabezpieczone metodą trwałego zapisu do pamięci nieulotnej.Macierz dyskowa musi posiadać funkcjonalność oszczędzania energii, w czasie niskiej aktywności procesory powinny pracować w trybie niskiego poboru mocy.Macierz dyskowa musi umożliwiać wymianę kontrolerów, kart rozszerzeń, dysków, zasilaczy i wentylatorów w trybie Hot Swap - w trakcie pracy pamięci dyskowej.Macierz dyskowa musi umożliwiać stosowanie dysków „Hot Spare” lub alternatywnie tzw. „przestrzeni spare” i wymianę dysków w trybie Hot Swap.Macierz dyskowa musi posiadać zainstalowaną pamięć cache DDR5 o sumarycznej pojemności fizycznej co najmniej **256GB**. Nie dopuszcza się użycia pamięci cache zbudowanej w formie dodatkowych, dedykowanych dysków SSD lub Flash, itp.Macierz dyskowa musi posiadać wbudowaną funkcjonalność szyfrowania dysków w standardzie AES 256.Pełna wewnętrzna redundancja kontrolerów, portów wewnętrznych, zasilania, chłodzenia i ścieżek danych na poziomie minimum N+1.Możliwość uaktualniania oprogramowania systemowego bez przerywania działania pamięci dyskowej, z utrzymaniem wszystkich funkcjonalności oraz z równoczesnym utrzymaniem dostępu do danych poprzez wszystkie ścieżki komunikacyjne Front-End z obydwu kontrolerów.Macierz dyskowa musi być wyposażona w system zapewniający bezpieczne, bez utraty danych, automatyczne wyłączenie w przypadku całkowitego zaniku zasilania.W przypadku awarii zasilania dane z pamięci cache muszą być zabezpieczone metodą trwałego zapisu do pamięci nieulotnej.Macierz dyskowa musi posiadać funkcjonalność oszczędzania energii, w czasie niskiej aktywności procesory powinny pracować w trybie niskiego poboru mocy.Macierz dyskowa musi umożliwiać wymianę kontrolerów, kart rozszerzeń, dysków, zasilaczy i wentylatorów w trybie Hot Swap - w trakcie pracy pamięci dyskowej.Macierz dyskowa musi umożliwiać stosowanie dysków „Hot Spare” lub alternatywnie tzw. „przestrzeni spare” i wymianę dysków w trybie Hot Swap.Macierz dyskowa musi posiadać zainstalowaną pamięć cache DDR5 o sumarycznej pojemności fizycznej co najmniej **256GB**. Nie dopuszcza się użycia pamięci cache zbudowanej w formie dodatkowych, dedykowanych dysków SSD lub Flash, itp.Macierz dyskowa musi posiadać wbudowaną funkcjonalność szyfrowania dysków w standardzie AES 256.Macierz dyskowa powinna posiadać możliwość szyfrowania wybranej grupy dysków lub wszystkich dysków w niej zainstalowanych.Macierz dyskowa musi obsługiwać standard NVMe w wersji co najmniej 1.4.Macierz dyskowa musi umożliwiać rozbudowę do co najmniej 72 dysków NVMe, bez użycia wirtualizacji innych macierzy.Macierz dyskowa musi umożliwiać rozbudowę do co najmniej 2,1PB surowej przestrzeni raw, otrzymanej z wewnętrznych dysków macierzy, bez użycia wirtualizacji innych macierzy.Macierz dyskowa musi umożliwiać instalację dysków wewnętrznych w standardzie minimum NVMe.Macierz dyskowa musi umożliwiać instalację następujących interfejsów sieciowych:Co najmniej 24 interfejsów FC, każdy o przepustowości co najmniej 64 Gbps.Co najmniej 16 interfejsów iSCSI, każdy o przepustowości co najmniej 25 Gbps.Co najmniej 8 interfejsów Ethernet (TCP), każdy o przepustowości co najmniej 100 Gbps.Dostarczone oprogramowanie i funkcjonalności muszą być udostępniane przez firmware bez modyfikacji przez Wykonawcę i jest to standardowe oprogramowanie producenta. Zamawiający nie dopuszcza takiej sytuacji, w której oprogramowanie pamięci dyskowej jest specjalnie przygotowane dla Zamawiającego.Macierz dyskowa musi posiadać mechanizmy kompresji i deduplikacji danych w trybie in-line.Macierz dyskowa musi posiadać funkcjonalność zdalnej replikacji danych w trybie synchronicznym i asynchronicznym za pomocą protokołu FC i iSCSI oraz replikację active-active typu Metro Cluster (równoległy dostęp do wolumenów z obydwu macierzy, w każdej parze replikacyjnej w trybie zapisu i odczytu). Oprogramowanie musi zapewniać funkcjonalność zawieszania replikacji i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zmiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora.Licencja na p Licencja na powyższą funkcjonalność nie jest częścią bieżącego postępowania.Macierz dyskowa musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point in time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym. Oferowane urządzenie musi obsługiwać minimum 500 000 kopii migawkowych (1024 per udział/dysk logiczny). Realizacja kopii migawkowych w trybie Copy-on-Write nie jest dopuszczona.Macierz dyskowa musi umożliwiać migrację dysków logicznych pomiędzy pulami dyskowymi w obrębie macierzy oraz pomiędzy przestrzenią zwirtualizowaną z innej macierzy, a przestrzenią wykreowaną z dysków wewnętrznych macierzy. Migracja odbywa się w trybie on-line bez przerywania pracy systemu/aplikacji korzystającej z danych migrowanego woluminu.Macierz musi umożliwiać konfigurację gwarancji wydajności typu QoS dla wybranych wolumenów logicznych w zakresie: wydajności w IOPS, wydajność w MB/s.Macierz dyskowa musi umożliwiać wirtualizację posiadanych przez Zamawiającego innych macierzy dyskowych. Jako wirtualizację definiuje się zabieg techniczny polegający na udostępnieniu wirtualizowanych wolumenów dyskowych klientom za pośrednictwem wirtualizatora. Mechanizm wirtualizacji musi być wbudowany w oprogramowanie wewnętrzne oferowanej pamięci dyskowej i nie może być realizowany z wykorzystaniem dodatkowych zewnętrznych urządzeń i oprogramowania.Wirtualizacja zasobów wewnętrznych poprzez możliwość partycjonowania zasobów i utworzenia przynajmniej 2 wirtualnych macierzy dla przynajmniej 2 hostów, z możliwością przydzielenia przestrzeni, portów.Nie jest dopuszczalne rozwiązanie, w którym usługi protokołu Fibre Channel realizowane są w oparciu o emulację protokołu FC na wewnętrznym systemie plików pamięci dyskowej.Jeśli jest to konieczne, wraz z pamięcią dyskową muszą zostać dostarczone licencje na funkcję kontrolerów umożliwiającą wykorzystywanie obu kontrolerów pamięci dyskowej w taki sposób, aby oprogramowanie zainstalowane w systemie operacyjnym klienta (serwera do wirtualizacji pamięci dyskowej) automatyczne przełączało ścieżki do zasobów, np. w przypadku uszkodzenia portu karty HBA, przełącznika SAN, kontrolera pamięci dyskowej czy przewodu światłowodowego.Dostarczane oprogramowanie zarządzające pamięcią dyskową oraz licencje umożliwiają:stałe monitorowanie stanu macierzy przez jej producenta z wykorzystaniem połączenia internetowego i protokołu HTTPS.informowanie o wykorzystaniu zasobów dyskowych macierzy m.in. całkowitej pojemności przestrzeni dyskowej macierzy, wykorzystanej przestrzeni dyskowej, skonfigurowanej przestrzeni przydzielonej do serwerów i nie przydzielonej do serwerów oraz przestrzeni nie skonfigurowanej (wolnej);monitorowanie zasobów wykorzystujących funkcjonalność thin-provisioning i ostrzeganie z wyprzedzeniem o możliwości wyczerpania zasobów;monitorowanie stanu pracy par replikacyjnych, kopii migawkowych i klonów oraz funkcjonalności klastra active-active;bieżące monitorowanie wydajności macierzy mierzonej w operacjach IOPS (zapis i odczyt), strumieniu MB/s (zapis i odczyt) oraz czasów odpowiedzi RT (zapis i odczyt) m.in. dla poszczególnych wolumenów logicznych, puli dyskowych oraz portów;przygotowywanie raportów historycznych z okresu co najmniej 12 miesięcy zawierających informacje o wydajności mierzonej w IOPS i MB/s dla poszczególnych wolumenów logicznych i puli dyskowych.wykrywanie błędów i izolowanie uszkodzeń, monitorowanie w czasie rzeczywistym.zarządzanie macierzą z graficznego interfejsu użytkownika (GUI), linii komend (CLI) oraz programowego REST API.monitoring i analizę wydajności systemu pamięci masowej (również macierzy firm trzecich), przełączników SAN oraz serwerów.monitorowanie parametrów wydajnościowych w zakresie co najmniej IOPS, MB/s oraz czasów odpowiedzi RT i raportowanie przekroczenia zdefiniowanych progów.korelację zmian parametrów wydajnościowych ze zmianami konfiguracji w środowisku.generowanie alertów dla administratora przez e-mail, SNMPwykorzystanie zewnętrznych serwerów uwierzytelniania użytkowników: MS AD/LDAPautomatyzacje zadań administracyjnych utworzoną w formie framework – graficznie przedstawienie zadań wykonywanych automatycznie zdefiniowany do uruchomienia poprzez wykrycie monitu (trigera).Automatyzowanie zmiany parametrów QOS dla wewnętrznej wirtualizacji zasobów udostępnianych do hostów/serwerówZarzadzanie oraz konfiguracja systemu kopii migawkowych wraz z repliką na inne ośrodki za pomocą GUI | |
|  | |

**1.2. Usługi wdrożeniowe**

W ramach rozbudowa środowiska wirtualnego o nową macierz dyskową, w tym migracji maszyn wirtualnych Wykonawca jest zobowiązany do :  
1.   Instalacja, okablowanie, uruchomienie i konfiguracja nowej macierzy,  
2.    Wystawienie zasobów z nowej macierzy do nowego klastra,  
3.    Wyłączenie maszyn starego klastra , ich migracja na nową macierz oraz na nowy klaster,  
4.    Migracja Live (Hyper-v Storage migration) - migracja na nową macierz bez wyłączania maszyn wirtualnych

na nowym klastrze  
5.    Uruchomienie zmigrowanych maszyn na nowym klastrze,  
6.    Rekonfiguracja posiadanej macierzy Fujistu i wykorzystanie jej jako zasób testowo-backupowy,  
7.   Demontaż 4 serwerów starego klastra.  
8.    Przygotowanie dokumentacji przed i powdrożeniowej.

**Część 2 Zamówienia :** Dostawa serwera do wirtualizacji wraz z systemem operacyjnym

**2.1 Dostawa serwera**

|  |  |
| --- | --- |
| **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
| **Obudowa** | Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość zamontowania ramienia do prowadzenia kabli. |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – 150W. Wymagana ilość rdzeni dla procesora – min 20. Minimalna częstotliwość pracy procesora 2.3GHz. Minimalna ilość kanałów procesora – 8 . Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 280 punktów int\_ base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org ([www.spec.org](http://www.spec.org)) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów. |
| **Liczba procesorów** | 2 |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje |
| **Pamięć operacyjna** | Zainstalowane minimum 512GB pamięci RAM o częstotliwości 3200MHz  Zainstalowana pamięć powinna być sygnowana i zoptymalizowana do użycia przez producenta serwera.  Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM przy użyciu pamięci RDIMM  Łączna ilość zainstalowanej pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 12TB |
| **Zabezpieczenie pamięci** | memory mirroring, ECC, SDDC, ADDDC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  1 port VGA na tylnym panelu serwera. |
| **Rozbudowa dysków** | W chwili dostawy serwer musi posiadać 8 zatok na dyski 2,5” w tym  W chwili dostawy serwer musi posiadać zainstalowane:   * Dwa dyski SSD SATA 2,5” o pojemności 480GB każdy. Dyski muszą mieć parametr DWPD min. 4 |
| **Kontroler dyskowy** | Zainstalowany sprzętowy kontroler SAS 12Gb, obsługujący poziomy RAID 0/1/10/5. Kontroler nie może zajmować żadnego ze slotów PCIe wyszczególnionych w „Dodatkowe sloty I/O” |
| **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. |
| **Interfejsy sieciowe** | Zainstalowane:   * Jedna dwuportowa karta sieciowa 10/25Gb SFP28 nie zajmująca żadnego ze slotów PCIe. Do karty należy dostarczyć dwie wkładki SFP28 10/25Gb. Karta musi wspierać protokół iWARP * Jedna dwuportowa karta sieciowa 10/25Gb. Do karty należy dostarczyć dwie wkładki SFP28 10/25Gb. Karta musi wspierać protokół iWARP * Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. |
| **Dodatkowe sloty I/O** | W chwili dostawy serwer powinien posiadać 3 sloty PCIe Gen4 PCIe z czego jeden x16. |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.1, 1x USB 2.0 * z tyłu obudowy: 2x USB 3.1, 1x VGA . Możliwość instalacji portu DB9 * wewnątrz obudowy: 1x USB3.1 |
| **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |
| **Zarządzanie** | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający:   * Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, plyta główna * Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O * Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. * Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. * Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 * Update systemowego firmware * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Zapis video zdalnych sesji * Podmontowanie lokalnych mediow z wykorzystaniem Java client * Przekierowanie kosnoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia systemu * Możliwość przejęcia zdalnego ekranu * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę * wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API * Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.   Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarządzanie infrastrukturą serwerów, przełączników i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń  - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych  - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia  - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,  - konsola zarzadzania oparta o HTML 5  - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,  - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja  - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania  - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń  - definiowanie roli użytkowników oprogramowania  - obsługa REST API oraz Windows PowerShell  - obsługa SNMP, SYSLOG, Email Forwarding  - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign-on oraz SAML  - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami  - przedstawianie historycznych aktywności użytkowników  -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych  - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem,  oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv  - Obsługa NTP  - przesyłanie alertów do konsoli firm trzecich  - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)  - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie  - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,  Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami:  VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms. |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM. Możliwość zainstalowana przedniego panelu zabezpieczającego zamykanego na klucz. |
| **Urządzenia hot-swap** | Dyski twarde, zasilacze, wentylatory. |
| **Obsługa** | Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser’ów PCIe, backplane’ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID  Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. |
| **System operacyjny** | Microsoft Windows Server 2025 x64 Datacenter PL lub produkt równoważny.  Za równoważność rozumie się zakup produktu obejmującego licencję systemu operacyjnego który zapewnia:   1. Współpraca z procesorami o architekturze x86 – 64bit. 2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. 3. Możliwość budowania klastrów składających się z 64 węzłów. 4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni. 5. Praca w roli klienta domeny Microsoft Active Directory. 6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016. 7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. 8. Możliwość uruchomienia roli klienta i serwera czasu (NTP). 9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 11. Możliwość uruchomienia roli serwera stron WWW. 12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. 13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. 14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). 15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:     1. pozwalają na zmianę rozmiaru w czasie pracy systemu,     2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,     3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,     4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość 19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 22. Możliwość wykorzystania standardu http/2. 23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 26. Mechanizmy logowania w oparciu o: a) login i hasło,     1. karty z certyfikatami (smartcard),     2. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:     1. określonych grup użytkowników,     2. zastosowanej klasyfikacji danych,     3. centralnych polityk dostępu w sieci,     4. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.     2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        * 1. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,          2. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,          3. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,          4. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,     3. zdalna dystrybucja oprogramowania na stacje robocze,     4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        * 1. Dystrybucję certyfikatów poprzez http,          2. Konsolidację CA dla wielu lasów domeny,          3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,          4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     6. szyfrowanie plików i folderów,     7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),     8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,     9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,     10. serwis udostępniania stron WWW,     11. wsparcie dla protokołu IP w wersji 6 (IPv6),     12. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     13. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),     14. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.     15. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover  z jednoczesnym zachowaniem pozostałej funkcjonalności.     16. mechanizmy wirtualizacji mające wsparcie dla:         * 1. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,           2. obsługi ramek typu jumbo frames dla maszyn wirtualnych.           3. obsługi 4-KB sektorów dysków,           4. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,           5. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.     17. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.     18. wsparcie dla rozwiązania Kubernetes.     19. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.     20. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).     21. mechanizmy deduplikacji i kompresji na wolumenach.     22. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.     23. mechanizm konfiguracji połączenia VPN do platformy Azure.     24. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.     25. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.     26. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard). |
| **Systemy operacyjne kompatybilność** | Microsoft Windows Server 2016, 2019, 2022, 2025 Red Hat Enterprise Linux 7, 8, 9 SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6, 7, 8, Ubuntu 18, 20, 22 |
| **certyfikaty** | 1. Urządzenie musi być wyprodukowane zgodnie z normą ISO 9001:2015 lub równoważną w zakresie co najmniej produkcji lub projektowania (odpowiedni dokument należy załączyć do oferty ). 2. Urządzenie musi być wyprodukowane zgodnie z normą ISO-14001 lub równoważną w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych. 3. Serwer musi posiadać deklarację CE lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym. (odpowiedni dokument należy załączyć do oferty ). 4. Serwer musi być wyprodukowany zgodnie z normą PN‑EN ISO 50001 lub równoważną potwierdzającą stosowanie w polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. |
| **Gwarancja** | 36 miesięcy gwarancji producenta on-site z czasem reakcji NBD. Możliwość wykupienia dodatkowego wsparcia z gwarantowanym czasem naprawy w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera. |

**2.2. Usługi wdrożeniowe**

W ramach rozbudowy klastra o kolejny host do wirtualizacji Wykonawca będzie zobowiązany do :  
1.    instalacja, okablowanie, uruchomienie i konfiguracja nowego serwera,  
2.    dodanie nowego serwera do klastra - rozbudowa klastra z 2 do 3 serwerów,  
3.    Przygotowanie dokumentacji przed i powdrożeniowej.

**Część 3 Zamówienia :** Dostawa systemu NAC

**3. Dostawa systemu NAC – 1 kpl**

**3.1 . Wymagane funkcjonalności 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 500 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 2 500 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 2016, 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 dostępu 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, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, 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 obsługę 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 urządzeniu, 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, minumum 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 (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    * Microsoft Windows
    * Mac OS
    * iOS
    * Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory 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 SNMP, DHCP, NMAP, 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 przesyłanie 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 wyłączania usług.

**Obsługa serwerów TACACS+**

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów 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, ostanie 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 nadam 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 wpierać 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 transkacji 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.

**3.2. Wymagania w zakresie usług konfiguracji oraz integracji.**

* Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
* Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
* Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
* Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
* Integracja posiadanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
* Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
* Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
* Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 30 dni po zakończeniu wdrożenia.

**3.3. Usługi szkoleniowe dla personelu Zamawiającego**

* Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC
* Warsztaty zostaną przeprowadzone dla max 7 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC
* Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC
* Warsztaty odbędą się w formie zdalnej .
* Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
* Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym

**3.4. Wymagania w zakresie wsparcia technicznego producenta oprogramowania**

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 24 miesięczną licencje 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.