Załącznik Nr 1a

Szczegółowy Opis Przedmiotu Zamówienia
Poprawa cyberbezpieczeństwa w Starostwie Powiatowym w Kępnie i wybranych jednostkach organizacyjnych II postępowanie

DYSKOWA MACIERZ WIODĄCA	
Parametr	Szczegółowy opis wymagania:
Obudowa	Obudowa typu Rack 19" – musi być dostarczona wraz z szynami do instalacji w szafie umożliwiającymi jej serwisowanie. Macierz musi być wyposażona w minimum 2 kontrolery Do urządzenia należy dołączyć kable połączeniowe zgodnie z ilością portów i rodzajem zainstalowanych modułów. Oferowane rozwiązanie musi zawierać się w obudowie o maksymalnej wysokości 2U
Funkcjonalności	Macierz musi umożliwiać wykonywanie procesu aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. Macierz musi umożliwiać **skalowalną rozbudowę on-line do minimum 8 kontrolerów** zarządzanych z jednej konsoli oraz poprzez dodawanie półek dyskowych do par kontrolerów. Po takiej rozbudowie musi być możliwość zaprezentowania każdego wolumenu logicznego LUN przez dowolny z kontrolerów bez przerywania dostępu do danych.
Kontrolery	Kontrolery macierzy muszą być wyposażone w co najmniej 192GB przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu. Kontrolery muszą wspierać jednocześnie ruch - **blokowy i plikowy** (wymagane protokoły: iSCSI, FC oraz plikowy CIFS - minimum SMB w wersjach 1,2,3,3.11 FTP i SFTP oraz NFS). Nie dopuszcza się realizacji funkcjonalności ruchu plikowego za pomocą dodatkowych/zewnętrznych urządzeń. Kontrolery te muszą działać w sposób redundantny – tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych – praca w trybie Active/Active. Macierz musi być odporna na awarię pamięci cache, w szczególności cache przeznaczony do zapisu (ang. Write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas. Uszkodzenie i wymiana pamięci Cache zapisu nie może powodować degradacji prędkości kontrolera. Wymiana pamięci Cache zapisu nie może powodować wyłączenia kontrolera macierzy. Każdy kontroler macierzy musi być oparty o wielordzeniowe procesory (minimum 20 rdzeni/kontroler) i pracować z częstotliwością minimum 2.4 GHz. Kontrolery **muszą współdziałać w trybie Active/Active**
Zasilanie	Urządzenie musi być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwany dostęp do wolumenów dyskowych (LUN) oraz działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
Przestrzeń dyskowa	Macierz musi zostać dostarczona w konfiguracji/wyposażona w przynajmniej: **17 dysków 2.5**" SSD NVMe Hot-Swap o pojemności minimum 3,84TB. Macierz musi umożliwiać **instalację minimum 4 dodatkowych dysków NVMe** bez dodawania półek, kontrolerów, czy innych elementów (jedynymi elementami dodawanymi jako rozbudowa muszą być same dyski)

	Dostarczona Macierz musi zapewnić przestrzeń użyteczną minimum 45 TiB (1TiB=1024GiB) Dostarczona Macierz musi zapewnić przestrzeń efektywną (po zastosowaniu mechanizmów kompresji i deduplikacji) minimum 90TiB Osiągnięta przestrzeń 90TiB musi być zapewniona i gwarantowana przez producenta macierzy. Macierz musi posiadać możliwość zapełnienia całej dostarczonej przestrzeni. Jeśli macierz pozwala na zapełnienie tylko części przestrzeni (np. 80%) to pozostająca „pusta- niewykorzystana" przestrzeń nie będzie wliczona w dostarczoną przestrzeń. Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie wydajności minimum 160 tysięcy IOPS z przestrzeni dyskowej (przy założeniach: dla bloku danych o wielkości 8k odczyt 70%, zapis 30% oraz wszystkie operacje losowe) Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie minimum 1300 MiB/s odczytu z przestrzeni dyskowej (nie z cache macierzy) W zaproponowanej konfiguracji macierzy należy także zabezpieczyć przestrzeń/dyski Hot/Spare według zaleceń producenta macierzy. Macierz w żadnej konfiguracji nie może oferować obsługi dysków obrotowych, a co za tym idzie nie może oferować rozbudowy o dyski obrotowe, czyli musi być rozwiązaniem zaprojektowanym tylko i wyłącznie do dysków SSD lub modułów flash. **Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy konfiguratora / estymatora – potwierdzony przez producenta, potwierdzający spełnienie powyższych wymagań (zawierający zarówno proponowaną konfigurację sprzętową z dokładnym wskazaniem part number'ów elementów jak i ich ilości, w tym typów i okresów wsparcia licencji i gwarancji) jak i wynikające z niej parametry pojemnościowe i wydajnościowe)**
Redukcja danych	Rozwiązanie musi zapewniać mechanizm kompresji i deduplikacji **danych w trybie in-line**. Kompresja i deduplikacja muszą być integralną częścią systemu macierzowego bez możliwości zatrzymania bądź wyłączenia przez administratora. Mechanizmy kompresji i dedpuplikacji muszą być przezroczysty dla administratora macierzy. Wobec powyższych wymagań dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne **dla wszystkich rodzajów przechowywanych danych** (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności). Wymagane jest zagwarantowane przez producenta oferowanej macierzy osiągnięcie współczynnika redukcji danych dla całej macierzy na poziomie 2:1 przy spełnieniu wymagań pojemnościowych określonych w punkcie Przestrzeń dyskowa. **Jeżeli producent nie gwarantuje współczynnika redukcji danych dla całej macierzy na poziomie 2:1, lub gwarantuje je w niższym stopniu, należy dostarczyć taką przestrzeń użyteczną, aby przestrzeń efektywna wynosiła 90TiB** W powyższej kalkulacji nie będzie wymagane uwzględnienie danych wcześniej zaszyfrowanych (z pominięciem mechanizmu szyfrowania przez macierz) i wcześniej skompresowanych.

	Zamawiający w momencie dostawy urządzenia wymaga przedstawienia zobowiązania producenta oferowanej macierzy gwarantującego uzyskanie oferowanego poziomu redukcji danych dla dostarczonej macierzy. W razie niedotrzymania oferowanej redukcji danych, producent zobowiąże się dostarczyć brakującą przestrzeń dyskową w oparciu o takie same nośniki, jak dostarczone inicjalnie z macierzą. Jeżeli takie zobowiązanie/umowa Producenta oferowanej macierzy nie zostanie przedstawiona Zamawiającemu do dnia odbioru przedmiotu zamówienia, zostanie to zinterpretowane jako brak wymaganego współczynnika redukcji danych.
Obsługa dysków	Macierz dyskowa musi umożliwiać stosowanie w niej na potrzeby składowania danych minimum następujących typów dysków: SSD SAS, SSD NVMe lub SCM. Dyski SCM muszą być wykorzystywane na przechowywanie danych. Niedopuszczalne jest użycie dysków SCM w szczególności jako rozszerzenia pamięci CACHE. Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność oferowanej macierzy.
Porty macierzowe front-end	Oferowane urządzenie musi być wyposażone w minimum: 2 porty 1Gbit przeznaczone do zarządzania macierzą 8 portów 10GbE SFP+ Musi być zapewniona możliwość rozbudowy macierzy o minimum 8 portów (FC 32Gb lub 25Gb iSCSI) jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów.
Porty macierzowe back-end	Oferowane urządzenie musi mieć możliwość wyposażenia w porty 100GbE do podłączenia dodatkowych półek dyskowych, aby umożliwić rozbudowę do min. 90 dysków.
Poziomy RAID	Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób, aby utrata dowolnego z nich zapewniła ciągłość dostępu do danych.
Kompatybilność	Rozwiązanie musi wspierać następujące środowiska wirtualne wykorzystywane przez Zamawiającego: VMware, MS Hyper-V, MS Windows, Linux, Oracle, aplikacje:, MS Exchange, MS SQL
Funkcjonalności	System musi obsługiwać natywną integrację z głównym środowiskiem wirtualizacyjnym Zamawiającego - VMware za pomocą interfejsu VAAI (VMware vStorage API for Array Integration), umożliwiając przypisanie do podsystemu pamięci masowej operacji VMware, takich jak wdrażanie pamięci masowej, klonowanie/snap i mechanizmu vMotion. Rozwiązanie musi łatwo integrować się z wirtualnymi środowiskami poprzez dostarczenie narzędzi do zarządzania i monitorowania. Rozwiązanie musi obsługiwać funkcję Local Protection (Snapshot z technologią Redirect-On-Write dla danych blokowych i plikowych i Thin Clones), rozwiązania, które nie obsługują funkcji redirect on write nie są dozwolone. Rozwiązanie powinno obsługiwać ciągłą ochronę danych dla VMware (z dowolnym odtwarzaniem point-in-time) Rozwiązanie musi obsługiwać kopie spójności aplikacji z replikacjami lokalnymi i zdalnymi Zamawiający nie wymaga dostarczenia licencji dla replikacji zdalnych na etapie postępowania. Rozwiązanie musi obsługiwać monitorowanie dla wydajności (Opóźnienie, IOPS, Odczyt/zapis, Szerokość pasma, Rozmiar IO, Długość kolejki), Pojemność (Łącznie, Oszczędność – redukcja danych, Snapshoty) i Konfiguracja z możliwością przekierowania powiadomienia na adres e-mail i łatwy dostęp poprzez aplikacje dostawców dla urządzeń mobilnych (Android i iOS). Rozwiązanie musi być hostowane w

	środowisku producenta macierzy i być udostępnione bez dodatkowych kosztów przez cały okres użytkowania proponowanego rozwiązania i zapewniać co najmniej 1 rok danych historycznych. **Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych** aplikacji w minimum wersjach: a) Exchange 2016 i 2019, SQL Server 2017 i 2019, Oracle 18 i 19, VMware dla blokowych i plikowych datastore. b) Spójność kopii rozumieć należy jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. c) Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. Macierz zarówno na poziomie jednej macierzy, jak i klastra – musi być zarządzana z poziomu jednej aplikacji, dostarczonej przez producenta urządzenia. Nie dopuszcza się dzielenia zarządzania pomiędzy różne aplikacje.
Replikacja	Rozwiązanie musi obsługiwać co najmniej dwukierunkową asynchroniczną zdalną replikację przez IP z opcją ustawienia relacji do: "1:1", "1:n", i "n:1".
	Macierz powinna oferować możliwość wykonania replikacji typu 3DC. Para wolumenów jest replikowana synchronicznie między ośrodkami i jednocześnie dodatkowo do trzeciego ośrodka musi istnieć możliwość replikacji w trybie asynchronicznym.
Funkcjonalność Storage Metro Cluster	Macierz powinna oferować możliwość replikacji wolumenu w trybie synchronicznym **minimum dla systemów Vmware**, w taki sposób, aby możliwy był jednoczesny zapis i odczyt z obu replikowanych wolumenów na obu macierzach w tym samym momencie. Dodatkowo w razie całkowitej utraty jednej z macierzy, powinny zadziałać mechanizmy wysokiej dostępności w taki sposób, aby dostęp do wolumenu był nieprzerwany z punktu widzenia serwerów korzystających z zasobów macierzy. Funkcjonalność musi być integralną cechą macierzy lub może być realizowana za pomocą dodatkowych urządzeń. Replikacja synchroniczna między macierzami musi odbywać się za pomocą protokołu IP lub FC.
	Musi istnieć taka możliwość konfiguracji macierzy dyskowych realizujących funkcjonalność Storage Metro Cluster, aby nie było konieczności używania tzw. świadka (Storage witness, Storage quorum, Storage tiebreaker).
	Funkcjonalność Storage Metro Cluster musi być realizowana w taki sposób, aby w przypadku całkowitej niedostępności jednej z macierzy dyskowych, ścieżki prezentowane do serwerów i obsługiwane przez multipathing były cały czas dostępne (status ACTIVE/ENABLED)
Thin Provisioning	Macierz musi zapewniać mechanizm thin provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą oferowaną pojemność macierzy.
Instalacja i szkolenie	Zamawiający wymaga, aby dostarczona macierz została zainstalowana i skonfigurowana przez certyfikowanego partnera producenta legitymującego się certyfikacją producenta na poziomie min. Platinium lub równoważny – certyfikat załączyć do oferty.
Gwarancja	Gwarancji producenta: 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 rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik wykonawcy / producenta z właściwym zestawem części do naprawy

	(potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	
	Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.
	
	Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.
	
	Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
	
	Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	
	Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.
	
	Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.
	
	Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia producenta, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	
	Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001:2017-06 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
	
	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
	
	Możliwość rozszerzenia gwarancji o:
	• Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:
	  o Monitorowanie zdarzeń w obrębie infrastruktury
	  o Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji
	• Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche)
	• Zdalne lub na miejscu wdrażanie poprawek - 2x w roku
	• Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)

Dodatkowe wymagania	**Dyski SCM nie mogą być przeznaczone/wykorzystywane wyłącznie do przechowywania metadanych bądź jako Cache** Rozwiązanie musi mieć możliwość rozbudowy do 448 rdzeni oraz minimum 10TB pamięci RAM. Rozbudowa nie może powodować wymiany zastosowanych dysków twardych.

	Pamięć Write Cache musi być mirrorowana (odpowiednik RAID1) nawet w razie awarii jednego z kontrolerów macierzy. Pamięć Write Cache musi być zabezpieczona dwoma bateriami – tak, aby w razie awarii jednej baterii, pamięć cały czas miała bateryjną ochronę Głębokość macierzy nie może przekroczyć 80cm
Szkolenia	Wykonawca przeprowadzi szkolenia z obsługi dostarczonej i wdrożonej infrastruktury przez autoryzowany personel. Wykonawca musi posiadać stopień autoryzacji producenta uprawniający do realizacji wdrożenia np. Platinum lub równoważny – załączyć do oferty

SIEM – system rozwiązań do analizy logów
Wartość wymagana:
1.Oprogramowanie musi pozwalać na monitorowanie sieci pod względem incydentów bezpieczeństwa (oprogramowanie typu NSM – Network Security Monitoring).
2. Oprogramowanie musi pozwalać na pełne przechwytywanie pakietów sieciowych oraz wykrywanie sieci i punktów końcowych (endpoints).
3. Przechwytywanie pakietów: Oprogramowanie musi pozwalać na:
a) przechwytywanie całego ruchu sieciowego;
b) automatyczne czyszczenie starych (archiwalnych) danych przed zapełnieniem zasobów dyskowych;
c) Generowanie i przechowywanie logi diagnostyczne;
d) przeglądanie pakietów za pomocą kwerend
4. Wykrywanie sieci i punktów końcowych: Oprogramowanie musi pozwalać na:
a) wykrywanie złośliwego, anomalnego lub podejrzanego ruchu w sieci na podstawie zestawu reguł;
b) wykrywanie włamań do sieci opartych na analizie ruchu w czasie rzeczywistym;
c) wykorzystanie agentów do monitorowania punktów końcowych w sieci (HIDS – Host-based Intrusion Detection System), w tym:
a. analiza dzienników systemowych;
b. monitorowanie zestawów predefiniowanych zasad;
c. wykrywanie rootkitów;
d. alarmowanie i reagowanie na incydenty w czasie rzeczywistym.
5. Oprogramowanie musi udostępniać graficzny interfejs WWW, który umożliwia:
a) dostęp jedynie zalogowanym użytkownikom (login oraz hasło);
b) podstawowy podgląd alertów bezpieczeństwa z systemów NIDS oraz HIDS;
c) rozszerzony podgląd alertów z określeniem miejsca zdarzenia oraz dokładnym opisem zdarzenia wraz z jego klasyfikacją;
d) wizualizację incydentów bezpieczeństwa w postaci graficznej (wykresów, diagramów);
e) interfejs do pełnego przechwytywania pakietów (PCAP – packet capture);
f) monitoring zasobów systemowych;
g) możliwość tworzenia własnych dashboardów oraz alertów
h) interfejs dla narzędzia pozwalającego na operację na danych pochodzących z alertów systemu;
6. Oprogramowanie musi pozwalać na niezależne wykorzystanie przynajmniej dwóch interfejsów sieciowych, w tym:
a) interfejs do zarządzania;

b) interfejs do nasłuchu ruchu sieciowego.
7. Oprogramowanie musi pozwalać na zarządzanie jego komponentami i przegląd zdarzeń systemowych za pomocą interfejsu konsolowego (CLI).
8. W zakresie zarządzania agentów HIDS oprogramowanie musi pozwalać na:
a) instalację agentów na urządzeniach z systemami Windows, MacOS, Linux;
b) rejestracja agentów poprzez REST API;
c) zarządzanie agentami poprzez interfejs konsolowy oraz REST API;
d) zabezpieczenie REST API z wykorzystaniem połączenia HTTPS;
e) tworzenie grup agentów i zdalne zarządzanie nimi;
f) zdalna aktualizacja agentów.
9. W zakresie HIDS oprogramowanie musi pozwalać na:
a) zbieranie danych z dzienników systemowych urządzenia agenta;
b) zbieranie informacji o systemie i jego zasobach;
c) monitorowanie integralności plików systemowych;
d) audyt zmian danych w systemie oraz przez kogo zostały dokonane;
e) wykrywanie anomalii i malware w systemie;
f) monitorowanie polityk bezpieczeństwa;
g) monitorowanie wykonywanych poleceń systemowych;
h) aktywne reagowanie na incydenty bezpieczeństwa – blokowanie dostępu do urządzenia dla intruzów;
i) „bezagentowy" monitoring urządzeń sieciowych poprzez SSH;
j) wykrywanie podatności w aplikacjach zainstalowanych na urządzeniu;
10. Oprogramowanie musi pozwalać na wizualizację zbieranych danych o incydentach bezpieczeństwa w postaci wykresów oraz posiadać predefiniowane zestawienia / kokpity (dashboards) i umożliwiać ich tworzenie z poziomu interfejsu graficznego WWW.
11. Oprogramowanie musi pozwalać na zbieranie logów za pomocą protokołu syslog
12. Oprogramowanie musi pozwalać na zdalne dodawanie nowych integracji przetwarzających logi z urządzeń: Palo Alto, Juniper, PulseSecure
13. Firma wdrażająca musi posiadać certyfikację ISO 27001:2017 - załączyć do oferty
14. Należy załączyć do oferty certyfikat potwierdzający wiedzę z zakresie bezpieczeństwa informacji i zarzadzania ryzykiem wydany przez uprawniony organ - min. Certified Information Systems Security Professional – CISSP - załączyć do oferty Wykonawca jest zobligowany do przeprowadzenia szkolenia dla personelu Zamawiającego.
15. Oprogramowanie musi obejmować moduł dot. systemu pomiarowego i zarządzania siecią spełniający poniższe wymagania:
Wymagania dla system pomiarowego i zarządzania siecią Wymagania dla Systemu pomiarowego i zarządzania siecią zwanego dalej Systemem zarządzania. System zarządzania musi poprawnie współpracować z przełącznikami dostarczanymi w ramach niniejszego postępowania. System zarządzania musi być dostarczony w postaci niezależnych instancji. Każda instancja (licencja jeżeli taki system jest stosowany przez producenta) musi obsługiwać co najmniej 1500 przełączników. System zarządzania musi składać się z dwóch elementów • Systemu konfiguracji i diagnostyki sieci (oprogramowania) • Stacji zarządzającej wraz z wizualizacją i zintegrowanym systemem do zarządzania siecią (zasoby sprzętowe)
Wymagania dla systemu konfiguracji i diagnostyki sieci 1) System zarządzania musi pozwalać na implementację oprogramowania w środowisku wirtualnym poprzez dystrybucję w postaci image docker oraz obraz maszyny wirtualnej. W przypadku obrazu maszyny wirtualnej dla systemu hostującego, wymagającego licencji, Wykonawca zobowiązany jest dostarczyć odpowiednie licencje.
2) System zarządzania musi posiadać Interfejs GUI dostępny z poziomu przeglądarki internetowej, działający przynajmniej z przeglądarkami Chrome i Firefox.
3) System zarządzania musi pozwalać na tworzenie indywidualnych kont użytkowników lokalnych lub uwierzytelnianych w usługach katalogowych (przynajmniej za pomocą protokołu LDAP). Ponadto musi pozwalać na rozróżnienie poziomu uprawnień indywidualnie dla każdego użytkownika z wyróżnieniem co najmniej praw do zarządzania innymi użytkownikami (user manager) i praw do

zarządzania mapami wizualizacji stanu sieci. a. System zarządzania musi wspierać opcję automatycznego logowania po restarcie platformy sprzętowej dla odpowiednich poziomów dostępu ReadOnly dla użycia w systemach wizualizacji
4) System zarządzania musi mieć możliwość ilustracji wielu warstw sieci w postaci hierarchicznych map i diagramów tworzonych przez administratora systemu manualnie np. Mapa_Kraju-> Mapa_Regionu->Mapa_Miasta->Schemat_sieci_Data_Center. System musi obsługiwać wykorzystanie jako tła (lub warstwy podkładowej) mapy geograficznej, na której są pozycjonowane urządzenia i połączenia pomiędzy nimi i na którym można wykorzystać pozycje GPS (np. OpenStreetMap). a. System zarządzania musi pozwalać na prace w trybie pełno ekranowym w którym mapa ilustrująca stan sieci zajmuje cały ekran z eliminacją pasków informacyjnych lub pól wyboru (menu) b. System zarządzania musi zapamiętywać ustawienia widoku personalne operatora systemu po to by po ponownym zalogowaniu operator widział analogiczne ustawienia widoków jak przed wylogowaniem
5) Przypisanie urządzeń do mapy musi być dostępne co najmniej w dwojaki sposób, indywidualnie konfigurowane dla każdego zmonitorowanych urządzeń: a. wsadowo poprzez wczytanie z pliku listy urządzeń dowiązanych do mapy z okresleniem: adresu IP, technologii komunikacji z urządzeniem (SNMP, NETCONF), koordynatów GPS, nazwy urządzenia, uwag/notatek oraz b. poprzez dodanie urządzenia do mapy z interfejsu GUI systemu zarządzania z podanie w/w parametrów.
6) System zarządzania musi pozwalać na oznaczanie urządzeń z poziomu GUI jako "zawieszone w monitorowaniu" tzw. tryb serwisowy polegający na wyróżnieniu takiego urządzenia specjalnym kolorem oraz zatrzymanie akcji związanych z monitorowaniem, ale pozostawienie na mapie w celu zachowania spójności diagramu sieci.
7) Urządzenia pozycjonowane na mapie wg. koordynat GPS muszą być lokowane w odpowiednich miejscach w celu ilustracji schematu sieci na mapie geograficznej
8) System zarządzania musi umożliwiać automatyczne wykrywanie połączeń interfejsów fizycznych pomiędzy urządzeniami na mapach i diagramach (wystarczająca jest realizacja tej funkcjonalności poprzez wykorzystanie uruchomionego na urządzeniach sieciowych protokołu LLDP).
9) System zarządzania musi wspierać monitorowanie urządzeń m.in. w celu pozyskania informacji na temat połączeń pomiędzy urządzeniami z wykorzystaniem protokołu SNMP i NETCONF
10) Wykrywanie nowych połączeń i ich ilustracja na mapie musi odbywać się automatycznie poprzez cykliczne skanowanie odpowiednich informacji z urządzeń monitorowanych. System musi obsługiwać konfigurację długości interwałów skanowania.
11) Wykryte łącza fizyczne pomiędzy urządzeniami muszą być ilustrowane na mapie (diagramie) w czytelny sposób m.in. stosując następujące techniki: a. Ilustracja łączy z wyróżnieniem łączy równoległych (tzw. multilink) pomiędzy urządzeniami, i podaniem ilości łączy w multilinku b. Ilustracja łączy z wyróżnieniem łączy agregowanych (tzw. LAG/trunk) pomiędzy urządzeniami, i podaniem ilości łączy w agregacie c. Ilustracja łączy z wyróżnieniem prędkości łącza i podaniem tej prędkości d. Ilustracja łączy z wyróżnieniem nieaktywnych łączy jako informacja historyczna e. Możliwość usunięcia manualnego z wizualizacji na mapie nieaktywnych połączeń f. Możliwość definiowania parametrów ilustrujących i wyróżniających łącze jak np. grubość linii zależnie od prędkości łącza g. Możliwość przypisania indywidualnie do urządzenia sposobu odczytywania parametrów stanu łączy i urządzenia przez protokoły SNMP lub NETCONF (z możliwością uwierzytelnienia dostępu ssh za pomocą klucza)
12) System zarządzania po wybraniu przez użytkownika na mapie/diagramie indywidualnego łącza musi pokazać informacje (np. w oddzielnym oknie) na temat Ilości łączy dla łącza zagregowanego, ilości aktywnych łączy, ich prędkości, nazwy interfejsów na urządzeniach na obu końcach łącza.
13) System zarządzania po wybraniu przez użytkownika na mapie/diagramie indywidualnego urządzenia musi pokazać informacje (np. w oddzielnym oknie) na temat nazwy urządzenia, adresu do zarządzania urządzeniem, modelu urządzenia, wersji oprogramowania, uwag dopisanych przez użytkownika np. o planowanych pracach utrzymaniowych, statusie urządzenia (np. czy jest w trakcie prac serwisowych)
14) W przypadku wystąpienia zdarzenia generującego Alarm na urządzeniu status urządzeń (poza urządzeniami w trybie "serwisowym") musi być ilustrowany na mapie w postaci łatwej do identyfikacji informacji (np. jako zmiana koloru ikony ilustrującej urządzenie). Po

	oznaczeniu na mapie takiego urządzenia musi być możliwość wyświetlenia bieżących alarmów na urządzeniu (np. w oddzielnym oknie lub karcie itd.).
15)	Monitorowanie zmian infrastruktury. System zarządzania musi śledzić informacje na temat wyposażenia każdego urządzenia indywidualnie (takie jak elementy składowe, moduły, wkładki). Śledzenie musi być realizowane min. poprzez cykliczne, w konfigurowanych przedziałach czasu, skanowanie wyposażenia urządzeń i zapisywanie ich. System zarządzania musi wyświetlać informację na temat zmian w wyposażeniu urządzeń pomiędzy dwoma dowolnymi krokami skanowania wyposażenia. Poprzez wyposażenie w szczególności dla urządzeń modularnych rozumiane są komponenty urządzenia, które według producenta danego urządzenia podlegają jednostkowej wymianie lub naprawie. Informacja dla każdego urządzenia musi zawierać min. numer modelu (ang. Part Number) i numer seryjny (ang. Serial Number).
16)	System zarządzania musi obsługiwać opcję zablokowania pozycji urządzeń na mapie.
17)	System zarządzania musi pozwalać na ilustracje na mapie ścieżki między dwoma urządzeniami (na podstawie protokołów routingu) z wyszczególnieniem ścieżek sygnalizowanych przez protokół LDP z uwzględnieniem ścieżek typu multipath
18)	System zarządzania musi pozwalać na ilustracje na mapie ścieżki między dwoma urządzeniami (na podstawie protokołów routingu) z wyszczególnieniem ścieżek sygnalizowanych przez protokół RSVP z uwzględnieniem ścieżek typu multipath
19)	System zarządzania musi pozwalać na ilustracje na mapie ścieżki między dwoma urządzeniami (na podstawie protokołów routingu) dla pakietów IPv4 oraz IPv6 z uwzględnieniem ścieżek typu multipath
20)	System zarządzania musi obsługiwać "zamrożenie" stanu sieci prezentowanego na mapie/diagramie bez nanoszenia zmian wynikłym z cyklicznego monitorowania w celu np. analizy stanu z danego momentu monitorowania.
21)	System zarządzania musi być zgodny i gotowy do natychmiastowego wdrożenia z oferowanymi urządzeniami.

Zasilacz awaryjny – UPS

Na wyjściu

Moc wyjściowa	5kW / 5.0kVA
Topologia	Technologia Double Conversion (On-Line)
Typ przebiegu	Sinusoida
Złącza wyjściowe	Połączenie poprzez zacisk 3-przewodowy (1fazowy+N+uziemienie)
Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą)	50/60Hz +/- 3 Hz
Inne napięcia wyjściowe	220, 240
Czas przełączania	0 s
Sprawność w trybie ECO	97%
Układ obejściowy (bypass) wewnętrzny	TAK

Na wejściu

Złącze wejściowe	Połączenie poprzez zacisk 3-przewodowy (1fazowy+N+uziemienie)
Częstotliwość wejściowa	40/70 Hz (automatyczne wykrywanie)
Zakres napięcia wejściowego w trybie podstawowym	170 – 300 V

Akumulatory i czas podtrzymania

Typ akumulatora	Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny
Typowy czas ładowania	4-5 godzin
Czas podtrzymania przy obciążeniu 100%	9 min
Czas podtrzymania przy obciążeniu 50%	22 min 34 sek
Automatyczny test akumulatora	Okresowy autotest akumulatora zapewnia wczesne wykrywanie

	konieczności wymiany.
Opcje przedłużonego podtrzymania zasilania	Rozszerzalny czas podtrzymania za pomocą 4 dodatkowych modułów akumulatorowych

Komunikacja i zarządzanie

Interfejs Port	Smart-Slot, Serial RS-232, USB (typ B)
Karta do zarządzania sieciowego	TAK
Awaryjny wyłącznik zasilania (EPO)	TAK
Panel sterowania	Wielofunkcyjna konsola sterownicza i informacyjna LCD.Tekst i schematy przedstawiające tryby działania, parametry systemu i alarmy.
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: ciągły sygnał dźwiękowy sygnalizujący przeciążenie

Ochrona przed przepięciami i filtracja

Klasa energetyczna sprzętu przeciwprzepięciowego	600J

Certyfikaty i zgodność z normami

Potwierdzenia zgodności	CE, IEC 62040-1-1, IEC 62040-1-2
Okres gwarancji	3 lata gwarancji na naprawę lub wymianę

Dodatkowe informacje

Możliwość montażu w szafie przemysłowej
Szyny do montażu w szafie przemysłowej (Rack) dołączone w zestawie
Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.