Załącznik nr 2a

Znak sprawy: RiiD.271.7.2025

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – Cześć 1

Spis treści

1 Wprowadzenie

1. Niniejszy dokument jest Opisem Przedmiotu Zamówienia dotyczącym kontumacji działań mających na celu wzmocnienie bezpieczeństwa systemów posiadanych przez Gminę Gnojnik
2. **Węzeł centralny** (WC) – Centrum przetwarzania danych, zlokalizowane u Zamawiającego zrealizowane w ramach grantu „Cyfrowa Gmina”.
3. **Klaster UTM** (KUTM) – Planowany zakup rozwiązania klasy UTM zmieniające urządzenie brzegowe obecnie wykorzystywane do chronienia Węzła Centralnego.
4. **Odmiejscowiona Kopia Zapasowa** (OKZ) – Planowane środowisko kopii zapasowej środowiska produkcyjnego WC zlokalizowane w innym budynku będącego w posiadani gminy. Pomiędzy budynkami w których zlokalizowany jest WC a budynkiem z OKZ zamawiający posiada połączenie światłowodowe.
5. **Środowisko Testowe** (ŚT) – Planowane odzwierciedlenie środowiska produkcyjnego zlokalizowane w budynku z OKZ. Połączenie ŚT z OKZ będzie ułatwiało testowanie aktualizacji środowisk produkcyjnych oraz będzie służyło do testowania w odizolowanym środowisku wykonanych kopii zapasowych systemów.
6. Zamawiający – Urząd Gminy Gnojnik.
7. Wykonawca – podmiot wybrany przez Zamawiającego do realizacji niniejszego zamówienia.
8. Użytkownik systemu – pracownik lub współpracownik Zamawiającego, pracownik jednostki organizacyjnej lub budżetowej Zamawiającego. Przez określenie „współpracownik” należy rozumieć osobę fizyczną, która nie jest zatrudniona u Zamawiającego na umowę o pracę, ale współpracuje z nim na zasadzie umowy zlecenia lub umowy o dzieło.
9. Pozostałe określenia użyte w opracowaniu należy rozumieć zgodnie z powszechnie akceptowaną nomenklaturą w dziedzinie problematyki objętej Zamówieniem.

Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, które wskazują lub mogłyby wskazywać na konkretnego producenta/dostawcę – nie stanowi to preferowania konkretnego wyrobu lub producenta/dostawcy, lecz ma na celu jedynie wskazanie cech – parametrów technicznych, użytkowych i jakościowych nie gorszych od podanych w opisie. Należy to więc traktować jedynie jako pomoc w opisie przedmiotu zamówienia. Podane w opisie nazwy własne mają na celu poinformowanie Wykonawców o zasobach, którymi dysponuje Zamawiający, aby zapewnić pełną kompatybilność oferowanych rozwiązań z istniejącą infrastrukturą. Zamawiający oczekuje, że dostarczone produkty i usługi nie będą generować dodatkowych kosztów związanych z koniecznością zakupu dodatkowego oprogramowania, sprzętu czy modyfikacji istniejących systemów.

Jeżeli Wykonawca stwierdzi, że użyte w opisie parametry lub normy krajowe lub przenoszące na normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to oznacza, że mają takie znaczenie, że parametry techniczne tak wskazanych produktów określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy. Wykonawca jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w opisie, również dopuszcza się wykazanie normami równoważnymi w stosunku do tych wskazanych w zapytaniu ofertowym. Na Wykonawcy spoczywa ciężar wykazania "równoważności”.

Wykonawca musi zaoferować spełniające min. takie wymagania i parametry techniczne, jak w opisie przedmiotu zamówienia. Wykonawca może zaoferować produkty o lepszych parametrach.

Dostarczone przedmioty zamówienia powinny być fabrycznie nowe, wykonane zgodnie z wymaganiami i normami mającymi zastosowanie do danego wyrobu, wolne od wad, odpowiadać normom jakościowym, określonym we właściwych aktach prawnych, posiadać aktualne aprobaty techniczne, gwarancje producenta oraz winny spełniać wszelkie wymogi przewidziane obowiązującymi przepisami dla tego typu wyrobów.

Poniższa specyfikacja obejmuje parametry techniczne minimum, jakie ma spełnić dostarczona infrastruktura.

2 Opis rozwiązania

1. Wymiana obecnie posiadanego urządzenia klasy UTM na Klaster UTM w trybie active-pasive podnoszące niezawodność działania systemów.
   1.1. Przy wymianie urządzeń planowane jest integracja z obecną infrastrukturą z odzwierciedlenia obecnie posiadanych ustawień (Loadbalance, pppoe, dhcp, vlan, polityki firewall, vpn).
   1.2. Kolejnym elementem zwiększenia bezpieczeństwa u zamawiającego będzie utwardzenie powyższych ustawień oraz włączenie i skonfigurowanie funkcjonalności/modułów wyspecyfikowanych w zamówieniu.
   1.3. Następnie zostanie uruchomienia klaster wysokiej dostępności urządzeń UTM oraz zasymulowanie awarii aktywnego urządzenia w celu sprawdzenia poprawności przełączenia się na urządzenie działające do tej pory w trybie pasywnym.
   1.4. W ramach części KUTM zostanie zakupiony system do agregowania logów, w celu agregowania i analizy logów z urządzeń i systemów Zamawiającego.
2. Stworzenie Odmiejscowionej kopii zapasowej będącej kolejnym elementem podnoszącym bezpieczeństwo środowiska produkcyjnego.
   2.1. Na środowisko OKZ składać będzie dedykowany serwer kopii zapasowej z oprogramowaniem oraz macierz dyskowa do duplikacji wykonanych kopii.
   2.2. Urządzenia będą zlokalizowane w innym budynku niż WC i połączone z infrastrukturą za pomocą koniecznych urządzeń aktywnych
3. Trzecią częścią zadania będzie zakup 2 serwerów z oprogramowaniem, które będzie symulować środowisko produkcyjne WC i będzie określane jako Środowisko Testowe.
   3.1. ŚT zostanie połączone z OKZ w wyodrębniony segmencie sieci do celów stworzenia wyizolowanego środowiska, w którym będą przeprowadzane testowanie aktualizacji/sprawność systemów oraz weryfikacji poprawności wykonanych kopii zapasowych

2.1 Środowisko instalacji i wdrożenia

1. Środowisko instalacji i wdrożenia u Zamawiającego
   1.1. Sprzęt i oprogramowanie dostarczane będą w lokalizacjach Zamawiającego:
      a. „Lokalizacja 1” – siedziba Zamawiającego w Gnojniku, 32-864 Gnojnik 363
      b. „Lokalizacja 2” – lokalizacja OKZ oraz ŚT oddalona nie więcej niż 1 km od lokalizacji głównej
   1.2. „Lokalizacja 1”: Zamawiający dysponuje klimatyzowaną serwerownią i miejscem w szafach RACK umożliwiającym zainstalowanie zamawianego KUTM. Serwerownia WC ulokowana jest na drugim piętrze budynku z szerokimi schodami.
   1.3. „Lokalizacja 2”: Lokalizacji posiada miejsce w szafie rakowej na OKZ, ŚT oraz połączenie światłowodowe z lokalizacją główną (dwa włókna). Serwerownia znajduje się na parterze.
2. Wszystkie prace niewymagające przerwy w pracy pracowników Zamawiającego mogą być realizowane w godzinach od 8 do 16 od poniedziałku do piątku.

3. Prace wymagające przerwy w pracy pracowników Zamawiającego mogą być realizowane po wcześniejszym uzgodnieniu z Zamawiającym, poza godzinami pracy Zamawiającego, które na dzień ogłaszania przetargu są następujące:
   - 7:30 – 16:30 – poniedziałek
   - 7:30 – 15:30 – od wtorku do czwartku
   - 7:30 – 14:30 – piątek
4. Dostarczone rozwiązanie zastąpi część urządzeń obecnie funkcjonujących u Zamawiającego, w związku z tym Wykonawca będzie musiał dostosować ich konfigurację (np. adresację IP) do rozwiązań obecnie stosowanych przez Zamawiającego. Oczekuje się, że przed wdrożeniem całego systemu Wykonawca zapozna się z konfiguracją urządzeń (np. UTM, przełączniki LAN itp.) funkcjonującą u Zamawiającego.
5. Przewidywany czas realizacji do 120 dni od podpisania umowy.

3 Wzmocnienie odporności cyfrowej Węzła Centralnego

3.1 Główne założenia projektowe

Węzeł Centralny zrealizowany przez zamawiającego w ramach grantu Cyfrowa Gmina służy zamawiającemu jako jednolite środowisko do wirtualizacji wraz z rozwiązaniami kopii zapasowej.

Obecne działania mają na celu wzmocnienie odporności poprzez wymianę obecnie posiadanego urządzenia brzegowego na odpowiednio wydajny KUTM.

Kolejnym elementem poprawiającym odporność cyfrową będzie wykonanie środowiska OKZ umiejscowione w „Lokalizacji 2”.

Trzecim elementem infrastruktury pomagającej w utrzymaniu sprawności całego środowiska przetwarzania będzie ŚT odzwierciadlające systemy posiadane w WC. Umiejscowienie ŚT zlokalizowane w „Lokalizacji 2” będzie też elementem możliwości szybkiego odtworzenia systemów krytycznych dla zamawiającego w monecie „Katastrofalnych awarii” Węzła Centralnego (pożar, katastrofa budowlana itp.).

ŚT będzie pracowało w wydzielonym segmencie sieci połączone z OKZ. Na ŚT będą testowane aktualizacji poszczególnych systemów WC oraz będzie służyło do weryfikowania poprawności wykonania kopii bezpieczeństwa poprzez przywracanie systemów z OKZ.

3.2 Celem niniejszego zadania jest:

1. Zabezpieczenie przed włamaniem i nieuprawnionym dostępem do danych (w tym do danych osobowych) dla środowiska WC, OKZ, ŚT oraz innych systemów informatycznych Zamawiającego.
2. Podniesienie poziomu bezpieczeństwa połączenia z siecią Internet (styku sieci WAN\LAN) poprzez zastąpienie dotychczasowych rozwiązań, funkcjonujących u Zamawiającego;
3. Uruchomienie i skonfigurowanie systemu zabezpieczenia danych (archiwizacja, backup, itp.).
4. Zbudowanie środowiska odwzorowujące WC w lokalizacji odmiejscowionej które będzie służyło do testowania wykonanych kopii zapasowych, testowania aktualizacji i wdrożeń nowych systemów oraz testowania zmian konfiguracyjnych w systemach produkcyjnych.
5. ŚT ma też służyć jako środowisko produkcyjne dla systemów krytycznych w przypadku katastrofalnej awarii WC. W przypadku awarii WC uniemożliwiającą pracę jakiegokolwiek systemu w ŚT zostaną odtworzone systemy krytyczne dla zamawiającego. Zamawiający przewiduje, że po wdrożeniu proponowanego rozwiązania czas pełnego odtworzenia pierwszego systemu krytycznego wraz z rekonfiguracją wymaganych urządzeń sieciowych nie będzie wynosiła więcej niż 6h, gdzie czas odtwarzania kolejnych systemy będzie już tylko czasem na przywrócenie maszyny wyturlanie w ŚT które przejmie zadania WC.

3.3 Oczekiwane rozwiązanie

1. KUTM będzie pierwszą linią obrony przed włamaniem i nieuprawnionym dostępem do danych. Dwa urządzenia UTM będą działać w trybie active-pasive. W przypadku awarii urządzenia aktywnego automatycznie urządzenie pasywne przejmie jego rolę. Synchronizacja ustawień pomiędzy urządzeniami oraz przełączenie ma odbywać się automatycznie bez żadnych ingerencji administratora. Urządzenia te będą terminować wszystkie vLANy wykreowane przez zamawiającego.
2. Łączność z Internetem jest zapewniona poprzez połączenia internetowe do 2 providerów internetowych działająca na zasadzie łącza zapasowego. KUTM ma być tak zorganizowany, aby przy awarii głównego łącza internetowego łącze zapasowe służyło do celów łączności internetowej dla pracowników i usług.
    1. Opisane w **Rozdziale 4** urządzenia klasy UTM zapewni Zamawiającemu bezpieczne połączenie z Internetem. Zastąpienie dotychczasowego rozwiązania klastrem UTM znacząco zwiększy niezawodność, a wyspecjalizowane funkcje urządzenia podniosą poziom bezpieczeństwa Zamawiającego.
3. OKZ opisane w **Rozdziale 5** będzie elementem zabezpieczenia danych umożliwiające wykonanie automatycznych kopii zapasowych WC. Wykonanych na dedykowanych urządzeniach z odpowiednim oprogramowanym oraz replikowanie kopii zapasowej na inne urządzenie magazynujące. Podstawowym warunkiem stawianym całemu rozwiązaniu jest możliwość:
    3.1. wykonywania kopii bez konieczności zatrzymywania jakiegokolwiek elementu całego systemu (środowiska wirtualnego, serwerów wirtualnych, baz danych, systemów dziedzinowych, czy aplikacji użytkowników);
    3.2. odtworzenia całego środowiska wirtualnego po awarii (Disaster Recovery);
    3.3. odtworzenie poszczególnych serwerów wirtualnych w sposób zapewniający spójność danych;
    3.4. odtworzenie poszczególnych plików w obrębie pojedynczego serwera wirtualnego;
    3.5. odtworzenie poszczególnych baz danych SQL, zachowując ich spójność;
4. **Rozdział 6** opisuje ŚT, które ma być odzwierciedleniem systemów WC na potrzeby testowania aktualizacji, testowanie zmian konfiguracyjnych środowiska produkcyjnego oraz testowania kopii zapasowych z OKZ. ŚT będzie się składało z 2 serwerów fizycznych z wymaganym oprogramowaniem tworzących klaster wysokie dostępności oraz uruchomieniu Usługi Katalogową.
    4.1. Klaster wysokiej dostępności (złożony z 2 serwerów) będzie mógł służyć do przywracania systemów z kopii zapasowej, testowania ich poprawności oraz testowania poprawności planowanych zmian konfiguracyjnych czy wdrażanych aktualizacji
    4.2. Uruchomiona Usługa Katalogowa będzie służyła do importu konfiguracji ze środowiska produkcyjnego i testowania utwardzeń polityk bezpieczeństwa.
    4.3. ŚT nie będzie odzwierciedlało całego zapotrzebowania Zamawiającego na potrzeby awarii katastrofalnych. Niemniej Zamawiający przewiduje, że w przypadku takowej awarii, systemy krytyczne zostaną przywrócone do działania w akceptowalnym czasie i z akceptowalną wydajnością. ŚT podczas prawidłowej pracy WC będzie służyło do wszelkiego rodzaju testów na systemach które nie będą w żadnym stopniu oddziaływać na WC

4 Lokalizacja 1 – Klaster UTM (KUTM)

1. Wykonawca dostarczy i skonfiguruje urządzenia 2 UTM które będą działać w klastrze active-pasive w taki sposób, aby zapewniały poziom bezpieczeństwa przynajmniej taki sam, jak obecnie jest stosowany przez Zamawiającego.
    1.1. Wykona w Lokalizacji 1 przełączenia obecnie funkcjonujące urządzenia UTM na nowo dostarczone. Po przełączeniu urządzeń, nie mogą przestać działać żadne usługi

informatyczne, dotychczas funkcjonujące u Zamawiającego (np. dostęp użytkowników do systemów IT z odległych lokalizacji, dostępność portali WWW udostępnianych przez Zamawiającego, poczta elektroniczna, łączność użytkowników z serwisami internetowymi voIP, itp.).

1.2. Na środowisku WC zainstalowanie i skonfigurowanie systemu do zbierania logów
   a. Wykonawca zasili system zbierania logów danymi z KUTM, oraz systemów wskazanych przez Zamawiającego.

1.3. Podczas pierwszego dnia szkolenia wdrożeniowego zostaną uruchomione dodatkowe moduły UTM zabezpieczeń, które zostały wyspecyfikowane w dalszej części dokumentu:
   a. Antywirus, spamBloker
   b. DDoS bloker
   c. IPS (Intrusion Prevention Service)
   d. AC (Application Controll)
   e. geolokalizacji (Geolocation Service)
   f. blokada ruch z systemami znajdującymi się na Czarnej liście NASK

1.4. Kolejne dni szkolenia zostaną przeznaczone na poznanie wdrożonej konfiguracji oraz sposobach jej zmieniania:
   a. Drugi dzień
      - Zarządzanie konfiguracją urządzeń (oraz omówienie ustawień globalnych)
      - Wykonywanie kopii zapasowej konfiguracji i jej przywracanie
      - Aktualizacja oprogramowania urządzeń wchodzących w skład klastra i odtwarzanie poprzedniej wersji (na wypadek niepowodzenia aktualizacja)
      - Integracja urządzeń z chmurą (kopia zapasowa, licencja)
      - Analiza logów i tworzenie powiadomień
   b. Trzeci dzień
      - Ustawienia sieciowe (konfiguracja vLAN, serwerów DHCP, stref DMZ, translacji NAT, konfiguracja interfejsów (WAN, tranków, bridgów, routingu statycznego),
      - VPN, przegląd i porównanie poszczególnych typów połączeń
      - Konfiguracja polityk (źródło, cel, usługa, port, zarządzanie polityką, ograniczenia zakresu i harmonogramu działania polityki, konfiguracja polityk dla protokołów VoIP)
   c. Czwarty dzień
      - Integracja z usługą AD i wykorzystywanie grup w politykach
      - Ograniczenia dostępu dla administratorów z poziomu wydzielonego segmentu sieci, awaryjny dostęp do urządzenia w przypadku awarii switach corowego

1.5. Maksymalny czas szkolenia wdrożeniowego to 4 dni po 5 godzin (szkolenie w trybie stacjonarnym).

1.6. Po wdrożeniu pełnej funkcjonalności KUTM zostanie zasymulowana awaria urządzenia aktywnego w celu weryfikacji automatycznego podjęcia pracy przez urządzenie pasywne.

2. Wykonanie wszystkich punków z poprzedniego akapitu 1, 1.1 – 1.6 będzie wymogiem podpisania protokół odbioru przedmiotu umowy.

4.1 Specyfikacja urządzeń UTM – 2 sztuki

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 2 szt. zapory sieciowej z pakietem bezpieczeństwa UTM pracujących w klastrze HA. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall jak i licencje na oprogramowanie UTM na minimum 36 miesięcy, usługi wdrożenia, szkolenia oraz wsparciem technicznego w języku polskim, dlatego wymagane jest uwzględnienie wszystkich elementów w ofercie.
Wymagania:

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3 oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC

(DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
27. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).
28. Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
29. Skaner antywirusowy ma pochodzić od europejskiego producenta.
30. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
31. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
32. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
33. Ochrona antyspam ma działać w oparciu o:
    33.1. białe/czarne listy,
    33.2. DNS RBL,
    33.3. Skaner heurystyczny.
34. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
35. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
36. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
37. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    37.1. PPTP VPN,
    37.2. IPSec VPN,
    37.3. SSL VPN.
38. SSL VPN ma działać w trybie tunelu.
39. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
40. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
41. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
42. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
43. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
44. Urządzenie ma posiadać wbudowany filtr URL.
45. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.

46. Administrator ma mieć możliwość dodawania własnych kategorii URL.
47. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    47.1. blokowanie dostępu do adresu URL,
    47.2. zezwolenie na dostęp do adresu URL,
    47.3. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
48. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
49. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
50. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
51. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
52. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
53. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
54. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    54.1. lokalną bazę użytkowników (wewnętrzny LDAP),
    54.2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    54.3. usługę katalogową Microsoft Active Directory.
55. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
56. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    56.1. SSL,
    56.2. Radius,
    56.3. Kerberos.
57. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
58. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
59. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
60. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
61. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
62. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
63. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
64. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

65. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    65.1. równoważenie względem adresu źródłowego,
    65.2. równoważenie względem połączenia.
66. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
67. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
68. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
69. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
70. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
71. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
72. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
73. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
74. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
75. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
76. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
77. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa poprzez zaszyfrowany protokół HTTPS.
78. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
79. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
80. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
81. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH).
82. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
83. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
84. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
85. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
86. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
88. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
89. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

90. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
91. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
92. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    92.1. manualnego eksportu do pliku w dowolnym momencie czasu,
    92.2. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
93. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
94. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
95. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
96. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
97. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
98. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
99. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
100. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
101. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
102. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
103. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
104. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
105. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
106. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
107. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
108. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
109. Urządzenie ma posiadać usługę DNS Proxy.
110. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
111. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
112. Urządzenie musi mieć zaimplementowane Open API.
113. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
114. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

115. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
116. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także muszą być objęte serwisem producenta w języku polskim.
117. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego rozwiązania, potwierdzające pochodzenie urządzeń z licencjami z oficjalnego kanału dystrybucyjnego producenta.
118. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
119. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
120. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. Razem z urządzeniem należy dostarczyć kartę microSD o pojemność min. 1TB.
121. Liczba portów Ethernet 2,5Gbps – min. 8.
122. Liczba portów światłowodowych 1Gbps – min. 1.
123. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
124. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.
125. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.
126. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.
127. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.
128. Liczba tuneli VPN IPSec – minimum 100.
129. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.
130. Obsługa interfejsów 802.11q (VLAN) – minimum 128
131. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę.
132. Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active-Passive.
133. Urządzenie nie ma limitu na liczbę użytkowników.
134. Liczba reguł filtrowania – minimum 8 192.
135. Liczba tras statycznego routingu – minimum 512.
136. Liczba tras dynamicznego routingu – minimum 10 000.
137. Urządzenie ma być dostarczone wraz z dodatkowym zewnętrznym zasilaczem (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
138. Urządzenie musi być wyposażone w moduł TPM.
139. Urządzenie ma być dostarczone z kompletem uchwytów do montażu w szafie rack 19”.

4.2 Specyfikacja Systemu wsparcia.

Razem z KUTM należy dostarczyć oprogramowanie do zbierania i analizy logów oraz reagowania na zagrożenia w celu kompleksowej ochrony infrastruktury IT. System musi bazować na nowoczesnych technologiach klasy SIEM (Security Information and Event Management), a także umożliwiać holistyczne podejście do bezpieczeństwa oraz zarządzanie incydentami w sposób wysoce zautomatyzowany i skalowalny. Oprogramowanie musi być w formie licencji wieczystej ze wsparciem technicznym na minimum 12 miesięcy. System należy wdrożyć na ŚT, a po konfiguracji zostanie migrowany do WC. Wymagania:

1. System musi gromadzić dane z różnorodnych źródeł, takich jak:

1.1. Logi systemowe (systemów operacyjnych, serwerów, aplikacji, urządzeń sieciowych).
1.2. Informacje o zdarzeniach (np. próby logowania, zmiany uprawnień, działania użytkowników).
1.3. Dane dotyczące konfiguracji infrastruktury IT (np. plików konfiguracyjnych, polityk bezpieczeństwa).

2. System musi automatycznie analizować dane w czasie rzeczywistym, identyfikując potencjalne zagrożenia oraz anomalie na podstawie wcześniej zdefiniowanych reguł, sygnatur oraz zaawansowanych algorytmów analitycznych.
3. Ciągłe monitorowanie stanu bezpieczeństwa w czasie rzeczywistym:
   3.1. Wczesne wykrywanie zagrożeń poprzez wykorzystanie analizy behawioralnej oraz sztucznej inteligencji do identyfikacji nietypowych zachowań użytkowników, urządzeń i aplikacji.
   3.2. Pełna widoczność nad wszystkimi elementami infrastruktury IT, w tym także nad środowiskami wirtualnymi i chmurowymi.
   3.3. Analiza historyczna zdarzeń: System musi umożliwiać retrospektywne badanie logów i zdarzeń, co jest niezbędne do dochodzeń powłamaniowych i audytów bezpieczeństwa.
4. System musi posiadać zaawansowane wykrywanie i reagowanie na zagrożenia w różnych środowiskach, takich jak:
   4.1. Środowiska chmurowe (AWS, Azure, Google Cloud).
   4.2. Kontenery (Docker, Kubernetes).
   4.3. Urządzenia końcowe.
5. System musi rozszerzać możliwości SIEM, pozwalając na:
   5.1. Skoordynowane wykrywanie zagrożeń w całym środowisku IT.
   5.2. Szybkie reagowanie na incydenty dzięki integracji z innymi narzędziami do zarządzania i automatyzacji (np. firewalle, narzędzia do zarządzania zasobami IT).
   5.3. Automatyzację działań naprawczych, co redukuje czas reakcji na zagrożenia oraz minimalizuje ryzyko.
6. System musi wspierać zarządzanie incydentami bezpieczeństwa poprzez:
   6.1. Automatyczne powiadomienia o wykrytych zagrożeniach, pozwalające administratorom na szybkie podjęcie działań.
   6.2. Raportowanie incydentów z pełnym zestawem informacji potrzebnych do analizy i dalszych działań naprawczych.
   6.3. Korelowanie zdarzeń z różnych źródeł w celu lepszego zrozumienia zagrożeń i zidentyfikowania ich źródła.
7. System musi pomagać organizacji w utrzymywaniu zgodności z regulacjami prawnymi i standardami bezpieczeństwa poprzez:
   7.1. Monitorowanie działań użytkowników i zapis zmian w systemach, co pozwala na śledzenie operacji oraz wykrywanie nieautoryzowanych działań.
   7.2. Automatyczne generowanie raportów audytowych i zgodności, które można przedstawić audytorom oraz organom nadzoru.
   7.3. Tworzenie alertów zgodności, które informują o potencjalnych naruszeniach polityk bezpieczeństwa.
8. System musi oferować wysoką skalowalność oraz zapewniać integrację z szeroką gamą innych rozwiązań i narzędzi używanych w ramach zabezpieczeń IT.

Razem z KUTM należy dostarczyć oprogramowanie do monitorowania infrastruktury IT, który zapewni kompleksową kontrolę nad zasobami sieciowymi, serwerami, aplikacjami oraz usługami IT. Oprogramowanie ma zapewnić pełne wsparcie dla operacji IT, wczesne wykrywanie problemów, automatyzację zadań oraz zapewnienie wysokiej dostępności i wydajności infrastruktury. System należy wdrożyć na ŚT, a po konfiguracji zostanie migrowany do WC. System musi być dostarczony z licencją bezterminową dla 50 hostów/adresów IP o poniższej funkcjonalności:

1. Monitorowanie serwerów i urządzeń sieciowych:

1.1. Możliwość monitorowania różnorodnych systemów operacyjnych (Windows, Linux, Unix).
1.2. Obsługa monitorowania urządzeń sieciowych (routery, switchy, firewalle).
1.3. Monitorowanie zasobów fizycznych (CPU, pamięć, dyski twarde).

2. Monitorowanie aplikacji i usług:
   2.1. Monitorowanie dostępności i wydajności aplikacji webowych oraz baz danych.
   2.2. Wsparcie dla monitorowania aplikacji chmurowych (AWS, Azure, Google Cloud).
   2.3. Możliwość monitorowania usług takich jak HTTP, HTTPS, FTP, SMTP, DNS itp.
3. Monitorowanie użytkowników i aplikacji www:
   3.1. Realizacja automatycznych testów pracy użytkownika w aplikacji www
   3.2. Monitorowanie wydajności aplikacji z perspektywy użytkownika końcowego.
   3.3. Kontrola międzyczasów podstron/kroków scenariusza pracy użytkownika aplikacji www.
4. Alertowanie i powiadomienia:
   4.1. Definiowanie progów alarmowych i automatyczne powiadamianie (e-mail, SMS, powiadomienia PUSH).
   4.2. Możliwość konfiguracji alertów w zależności od krytyczności incydentu.
   4.3. Integracja z systemami zarządzania incydentami (ITSM).
   4.4. Eskalacja powiadomień
5. Raportowanie i analiza danych
   5.1. Generowanie raportów dotyczących dostępności, wydajności oraz wykorzystania zasobów.
   5.2. Wizualizacja danych w postaci wykresów i dashboardów.
   5.3. Możliwość eksportu raportów do formatów takich jak PDF, CSV.
   5.4. Tworzenie i modyfikacja raportów za pośrednictwem interfejsu WWW bez konieczności instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash itp.).
   5.5. Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów według zdefiniowanego harmonogramu, możliwość generowania raportów dostępności (wg hostów lub usług), raportów SLA (wg hostów lub usług), raportowanie incydentów, awarii itp., raportowanie wydajności sieci, zapis raportów do plików PDF, okresowe wysyłanie raportów e-mailem do wskazanych użytkowników, powiadomienia e-mail o incydencie, zapis zdefiniowanych parametrów raportów celem późniejszego wywołania.
6. Automatyzacja i orkiestracja
   6.1. Automatyczna konfiguracja nowych urządzeń
   6.2. Automatyczne wykonywanie skryptów w odpowiedzi na zdarzenia.
   6.3. Integracja z narzędziami do zarządzania konfiguracją (Ansible, Puppet, Chef).
   6.4. Możliwość definiowania i uruchamiania zadań uwzględniając harmonogram dni i godzin.
7. Bezpieczeństwo i audyt
   7.1. Zapewnienie szyfrowanej komunikacji między komponentami systemu.
   7.2. Monitorowanie i audytowanie zdarzeń związanych z bezpieczeństwem.
   7.3. Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi).
   7.4. Wbudowany mechanizm zarządzania użytkownikami systemu.
   7.5. Możliwość tworzenia grup użytkowników.
   7.6. Historia danych statystycznych.
   7.7. Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
   7.8. Audyt pracy użytkownika w systemie
8. Integracje i API
   8.1. Otwarte API umożliwiające integrację z innymi systemami.
   8.2. Wsparcie dla integracji z popularnymi narzędziami do zarządzania IT (np. ServiceNow, Jira).

8.3. Natywna integracja z systemami do centralnego gromadzenia logów i analizy zdarzeń opartymi o architekturę Elasticsearch, Opensearch
8.4. Natywna integracja z systemami klasy SOAR
8.5. Możliwość korzystania z webhooków do przesyłania danych w czasie rzeczywistym.
8.6. Możliwość konfiguracji oprogramowania poprzez stronę www oraz programistyczne, udokumentowane API.

9. Interfejs użytkownika
9.1. Interfejs graficzny do wizualizacji struktury sieci.
9.2. Interfejs graficzny do wizualizacji poszczególnych wybranych parametrów urządzeń.
9.3. Przyjazny i intuicyjny interfejs webowy dostępny z poziomu przeglądarki.
9.4. Możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu oraz dowolnej konfiguracji składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget'ów.
9.5. Możliwość tworzenia wielu dashboardów
9.6. Możliwość tworzenia dashboardów prywatnych jak i współdzielonych pomiędzy innymi użytkownikami aplikacji
9.7. Możliwość tworzenia dashboardów typu iFrame – będącymi oknem aplikacji zewnętrznych
9.8. Możliwość tworzenia własnych dodatków do dashboardów w formie obiektów programistycznych typu Widget. Aplikacja musi wspierać dodawanie własnych rozszerzeń do dashboardów.
9.9. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień push.
9.10. Możliwość tworzenia i zapisywania filtrów dla monitorowanych urządzeń i ich parametrów
9.11. Możliwość wykorzystania filtrów podczas tworzenia dashboardów
9.12. Monitorowanie specyficznych parametrów i elementów infrastruktury:
9.13. Monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałych parametrów działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta).
9.14. Możliwość monitorowania aplikacji i procesów o dynamicznym zachowaniu.
9.15. Możliwość monitorowania min. krytycznych elementów infrastruktury, aplikacji, usług sieciowych, protokołów sieciowych, wskaźników systemowych, infrastruktury sieciowej, portów.
9.16. Możliwość śledzenia parametrów takich jak:
a. Telnet na wybrany port – nasłuch na porcie,
b. Ping dostępność urządzenia,
c. Odczyt, przetwarzanie i generowanie alertów z pułapek SNMP,
d. Poprawne działanie serwera DHCP,
e. Poprawne działanie serwera czasu NTP,
f. Zajętość danych na poszczególnych partycjach,
g. Zajętość RAM,
h. Obciążenie systemu,
i. Obciążenie dysków,
j. Ilość zalogowanych użytkowników,
k. Ilość procesów,
l. Obecność procesów w systemie,
m. Synchronizacja dysków programowego RAID,
n. Synchronizacja dysków sprzętowego RAID,
o. Kontrola parametrów polecenia VMSTAT,
p. Obecność SSH.
9.17. Możliwość śledzenia parametrów monitoringu systemu poczty:

a. Poprawne działanie serwera SMTP,
b. Poprawne działanie serwera POP3,
c. Poprawne działanie serwera IMAP,
d. Ilość listów w kolejkach serwera Postfix.

9.18. Możliwość śledzenia parametrów monitoringu DNS:
a. Poprawne działanie DNS,
b. Rozwiązywanie zadanych domen na adresy IP,
c. Parametry serwerów WWW,
d. Poprawne działanie serwera WWW,
e. Kontrola występowania oczekiwanych treści na stronie,
f. Czas odpowiedzi serwera WWW.

9.19. Możliwość śledzenia parametrów monitoringu bazy danych:
a. Poprawna praca bazy,
b. Kontrola stanu synchronizacji baz,
c. Zajętość przestrzeni danych.

9.20. Możliwość śledzenia parametrów DRBD i HEARTBEAT:
a. Poprawne działanie klastra,
b. Poprawne działanie replikacji danych.

9.21. Możliwość śledzenia parametrów macierzy dyskowych:
a. Analiza statusów ogólnych urządzenia,
b. Analiza dysków urządzenia.

10. Dodatkowe Elementy Infrastruktury Informatycznej do Monitorowania
10.1. Monitorowanie zasobów wirtualnych (maszyny wirtualne, hypervisory).
10.2. Monitorowanie infrastruktury kontenerowej (Docker, Kubernetes).
10.3. Monitorowanie systemów backupowych i urządzeń magazynujących.
10.4. Monitorowanie systemów IoT i urządzeń edge computing.
10.5. Monitorowanie systemów SCADA i przemysłowych systemów sterowania.
10.6. Monitorowanie infrastruktury zasilania (UPS, generatory).
10.7. Monitorowanie systemów HVAC (Heating, Ventilation, and Air Conditioning).
11. Architektura Systemu
11.1. System musi działać w modelu klient-serwer.
11.2. System pracuje pod kontrolą środowiska systemu operacyjnego Open Source.
11.3. Możliwość wdrożenia systemu zarówno on-premises, jak i w chmurze.
11.4. Wsparcie dla skalowalności poziomej i pionowej.
11.5. System musi wspierać architekturę wysokiej dostępności dla każdej warstwy systemu.
11.6. System musi umożliwić rozbudowę, pozwalającą na monitorowanie nieograniczonej wydajnością liczby urządzeń w sieci. Architektura musi umożliwiać rozkładanie obciążenia pomiędzy elementy systemu.
12. Wymagania dotyczące składowania danych
12.1. Możliwość replikacji i backupu danych.
12.2. Gromadzone dane muszą musza być składowane w nierelacyjnej bazy danych.
13. Wymagania dotyczące zgodności
13.1. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień.
14. Dostępność szczegółowej dokumentacji technicznej w języku polskim dla administratorów systemu.

4.3 Zakres prac wdrożeniowych:

1. Analiza przedwdrożeniowa:
a. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
b. Opracowanie planu wdrożenia.
2. Wdrożenie i konfiguracja:

a. Instalacja urządzeń UTM oraz podłączenie do sieci.
b. Konfiguracja przełącznika zgodnie z wymaganiami zamawiającego.
c. Integracja z istniejącymi systemami IT zamawiającego.

3. Testy akceptacyjne:
   a. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
   b. Weryfikacja poprawności działania przełącznika.

5 Lokalizacja 2 – Odmiejscowiona Kopia Zapasowa (OKZ)

1. W ramach realizacji OKZ zadania wykonawca dostarczy i skonfiguruje w Lokalizacji 2 wskazanej przez zamawiającego następujące elementy tworzące w całości OKZ:
   1.1. Przełącznik sieciowego (**PS**)
   1.2. Serwer odmiejscowionej kopii zapasowej dla WC (**SOKZ**)
   1.3. Oprogramowanie do tworzenia kopii zapasowi WC które zostanie zainstalowanie na urządzeni **SOKZ**
   1.4. Urządzenie macierzowe do replikacji kopii zapasowej z **SOKZ**
2. Zakup, dostawa i konfiguracja **PS** ma służyć komunikacji **OKZ** z WC oraz separacji i organizacji współpracy ze **ŚT**.
3. W zakresie uruchomienia i skonfigurowania systemu **OKZ**, planuje się zakupić sprzęt i oprogramowanie umożliwiające wykonywanie automatycznych kopii zapasowych środowiska WC w systemie „disk-to-disk”. Podstawowym warunkiem stawianym całemu rozwiązaniu jest możliwość:
   3.1. wykonywania kopii bez konieczności zatrzymywania jakiegokolwiek elementu całego systemu (środowiska wirtualnego, serwerów wirtualnych, baz danych, systemów dziedzinowych, czy aplikacji użytkowników);
   3.2. odtworzenie poszczególnych serwerów wirtualnych w sposób zapewniający spójność danych;
   3.3. odtworzenie poszczególnych plików w obrębie pojedynczego serwera wirtualnego;
   3.4. odtworzenie poszczególnych baz danych SQL, zachowując ich spójność.
   3.5. Powyższe dane muszą też zostać (automatycznie lub wg. harmonogramu) replikowane na urządzenie macierzowe pracujące w tym samym segmencie sieci
   3.6. Skonfiguruje port do zdalnego zarządzania serwerem dla każdego z zakupionych serwerów.
   3.7. Po zakończeniu wykonywania kopii zapasowej (niezalenie czy zakończono z błędem czy bez) ma zostać wysłany mail na adres wskazany przez Zamawiającego).
   3.8. Skonfiguruje port do zdalnego zarządzania dla każdego z zakupionych urządzeń.
4. Wykonanie punktów pkt. 3.1 do pkt. 3.8 na działającym „Węźle Centralnym” będzie wymogiem podpisania protokół odbioru przedmiotu umowy.

5.1 Specyfikacja przełącznika sieciowego (PS)

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
   2.1. możliwość montażu w stelażu/szafie 19”
   2.2. wysokość maksymalna 1U

2.3. głębokość urządzenia nie większa niż 40 cm
2.4. waga urządzenia nie większa niż 5 kg
2.5. dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Urządzenie musi zostać dostarczone z 2 zasilaczami z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap) oraz z 2 kablami zasilającymi o długości min. 2m.
2.6. zakres temperatur pracy ciągłej co najmniej od 0 do +45 °C
2.7. zakres wilgotności pracy co najmniej 5% – 95%
2.8. maksymalny pobór mocy nie większy niż: 100W

3. Przepływ powietrza przód-tył (od strony portów w kierunku zasilaczy)
4. Urządzenie musi być wyposażone w 2 wentylatory.
5. Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie:
   5.1. 16 portów 1/10GE SFP+ wyposażone w 16 modułów SFP+ 10G MM oraz 16 patchcordów długości 3m
   5.2. 8 portów 1/2.5/5/10G BASE-T Ethernet
6. Wszystkie porty 1/10G SFP+ muszą być dostępne od frontu urządzenia.
7. Możliwość zmiany karty rozszerzeń w poniższych opcjach:
   7.1. 2 porty 10G SFP+ z MACSec
   7.2. 2 porty 10G BASE-T z MACSec
   7.3. 8 portów 10G SFP+ z MACSec
   7.4. 4 porty 10/100/1000BASE-T Ethernet oraz 6 portów SFP
   7.5. 2 porty 25GE SFP28
   7.6. 2 porty 40GE QSFP+
8. MTBF min. 500 tys. godzin.
9. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
   9.1. Zarządzanie stosem poprzez jeden adres IP
   9.2. Do min. 9 jednostek w stosie
   9.3. Porty do stackowania mogą być współdzielone z portami typu uplink.
   9.4. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
   9.5. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
   9.6. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
10. Zamawiający dopuszcza aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink.
11. Układ przełączający o wydajności min. 480Gbps, wydajność przełączania przynajmniej 350 Mpps
12. Obsługa min. 32 700 adresów MAC
13. Wbudowana pamięć RAM min. 2 GB
14. Procesor wielordzeniowy. Minimalne taktowanie procesora 1600MHz
15. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
16. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
17. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie.
18. Obsługa ramek jumbo o wielkości min. 9216 bajtów
19. Obsługa protokołu BFD oraz LACP
20. Obsługa protokołu VRRP dla IPv4 i IPv6
21. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
22. Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania

23. Obsługa min. 16 000 tras dla routingu IPv4
24. Obsługa min. 8 000 tras dla routingu IPv6
25. Obsługa min. 10 000 IPv6 neighbor discovery (ND)
26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
    26.1. IGMP v1, v2 i v3
    26.2. IGMP Snooping v2 i v3
    26.3. PIM-SM, PIM-SSM i PIM-DM
    26.4. MSDP i MLD Snooping
    26.5. minimum 4000 tras multicast dla IPv4 i minimum 2000 tras multicast dla IPv6
27. Minimalny rozmiar tablicy ARP 16 000 wpisów
28. Obsługa protokołów LLDP i LLDP-MED.
29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
30. Obsługa sFlow
31. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    31.1. min. 3 poziomy dostępu administracyjnego poprzez konsolę
    31.2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
    31.3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    31.4. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
    31.5. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
    31.6. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
    31.7. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
    31.8. obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection, Root Protection, Loop Protection
    31.9. możliwość synchronizacji czasu zgodnie z NTP lub SNTP
32. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
    32.1. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
    32.2. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
33. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
34. Wsparcie dla funkcjonalności VXLAN L2 i L3. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający wymaga jej dostarczenia.
35. Wsparcie dla technologii MPLS, w tym L3 VPN. Jeżeli funkcjonalność MPLS wymaga licencji to należy ją dostarczyć w ramach niniejszego postępowania
36. Wsparcie dla funkcjonalności M-LAG lub MC-LAG
37. Wsparcie dla funkcjonalności DCBx oraz PFC
38. Wymagane opcje zarządzania:
    38.1. możliwość lokalnej obserwacji ruchu na określonym porcie
    38.2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
    38.3. wsparcie dla skryptów python uruchamianych na urządzeniu
    38.4. wsparcie dla RMON
    38.5. dedykowany port konsoli, zgodny ze standardem RS-232
    38.6. dedykowany port zarządzający out-of-band Ethernet 10/100Base-T
39. Wraz z urządzeniami muszą zostać dostarczone:
    39.1. pełna dokumentacja w języku polskim lub angielskim

39.2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE) lub równoważne potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym, lub oświadczenie, że deklaracja nie jest wymagana

40. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 9 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
41. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
42. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
43. Usługa serwisu musi być świadczona w języku polskim.
44. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
45. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
46. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
47. System centralnego zarządzania może być dostarczony w formie:
    47.1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
    47.2. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
48. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
49. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
50. System centralnego zarządzania musi umożliwiać:
    50.1. tworzenie VLANów
    50.2. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
    50.3. tworzenie połączeń zagregowanych
    50.4. monitorowanie statusu pracy przełącznika i portów
    50.5. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
    50.6. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
    50.7. interfejs do zarządzania w języku polskim lub angielskim

5.2 Specyfikacja SOKZ

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 12 dysków 3,5”. Serwer musi posiadać możliwość rozbudowy o 4 dodatkowe wnęki dyskowe na dyski SAS/SATA/NVMe 2.5”.
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz wyposażeniem w przedni panel zamykany na klucz, chroniącym dyski przed nieuprawnionym wyjęciem.

3. Płyta główna z możliwością zainstalowania do dwóch procesorów.
4. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5. Zainstalowane dwa procesory piątej generacji min. 16-rdzeniowe o taktowaniu min. 2.0GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów min. 420 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 256 GB RAM DDR5 RDIMM 5600MT/s, w modułach po 64 GB RAM.
7. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
8. Zabezpieczenie pamięci:
    a. Memory mirroring
    b. ECC
    c. patrol scrubbing
    d. SDDC
    e. memory thermal throttling
    f. ADDDC-SR
    g. PPR
    h. Memory SMBus hang recovery.
9. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
10. Wbudowane porty:
    a. min. 4 porty USB z czego nie mniej niż 1 x USB 3.0 na przednim panelu obudowy, 2 x USB 3.0 na tylnym panelu obudowy oraz 1 x USB 2.0 na płycie głównej;
    b. dodatkowo złącze USB TYP-C na przednim panelu, które musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS;
    c. port VGA na tylnym panelu obudowy;
    d. powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
11. Minimum 3 aktywne sloty PCI-E 5.0 z czego min 1 slot x16.
12. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,
    b. minimum 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ Multimode
    c. minimum 4 porty 1Gb/s Ethernet w standardzie Base-T
    d. powyższe porty nie może zajmować slotów PCI-E.
13. Pamięć masowa:
    a. zainstalowane 2 dyski serwerowe SSD M.2 Read-Intensive Hot-Plug o pojemności min. 480 GB każdy. Dyski muszą być skonfigurowane w RAID1 przez dedykowany kontroler sprzętowy i nie mogą zajmować kieszeni na dyski 3.5”.
    b. zainstalowane 3 dyski serwerowe SSD SATA o pojemności min. 1.92 TB każdy.
    c. zainstalowane 6 dysków serwerowych HDD SATA 7.2K o pojemności min. 8 TB każdy.
14. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
15. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
16. Min. dwa identyczne zasilacze o mocy min. 1600W klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera. W komplecie z zasilaczami należy dostarczyć kable zasilające o długości min. 2m.
17. Bezpieczeństwo:
    a. wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. moduł TPM 2.0.

18. Możliwość wyposażenia serwera w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:
    a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS
    b. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy
    c. przywracanie konta administratora
    d. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera
    e. wyświetlanie w czasie rzeczywistym temperatury procesorów
    f. konfigurowanie ustawień sieciowych modułu zarządzania.
19. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:
    a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),
    b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer,
    c. zbieranie logów błędów hardware,
    d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,
    e. montowanie wirtualnych napędów,
    f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,
    g. wysyłanie zawiadomień droga mailową i poprzez SNMP
    h. wsparcia dla IPMI, SSH, Redfish
    i. wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,
    j. nadawanie ról użytkownikom,
    k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,
    l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.
20. Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    a. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.
    b. tworzenie szablonów instalacyjnych dla systemów operacyjnych.
    c. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.
    d. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.
    e. aktualizacja sterowników i BIOS serwerów.
    f. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
21. Zgodność z normami:
    - ISO 9001 lub równoważne zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami
    - ISO 14001 lub równoważny spełniający wymagania związane z zarządzaniem środowiskowym, zgodnością z przepisami, ciągłym doskonaleniem na rzecz ochrony środowiska, monitorowaniem wpływu na środowisko.
    - ISO 27001 lub równoważny spełniający wymagania dotyczące zarządzania bezpieczeństwem informacji, ochrony danych i zarządzania ryzykiem

- ISO 50001 lub równoważny zapewniający zarządzanie efektywnością energetyczną, ciągłe doskonalenie procesów energetycznych i zgodność z przepisami prawnymi dotyczącymi ochrony środowiska

22. Serwer musi posiadać deklarację CE lub równoważne potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym.
23. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
24. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
25. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem w języku polskim
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.
    c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.
    e. Usługi gwarancyjne świadczone przez producenta lub autoryzowanego partnera serwisowego producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami.
    f. Wymaganie oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
    g. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
        i) możliwość pobierania najnowszego firmware,
        ii) dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
        iii) dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
        iv) otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

5.3 Specyfikacja oprogramowania do tworzenia kopii zapasowej WC.

Poniżej wyspecyfikowane oprogramowanie zostanie na urządzeniu wyspecyfikowanym Rozdziale 5.2 Specyfikacja SOKZ

1. Wykonywanie automatycznych kopii zapasowych całego środowiska wirtualnego (minimum 20 maszyn wirtualnych).
2. Wykonywania kopii zapasowych bez konieczności zatrzymywania jakiegokolwiek elementu całego systemu (środowiska wirtualnego, serwerów wirtualnych, baz danych, systemów dziedzinowych, czy aplikacji użytkowników).
3. Możliwość odtworzenia całego środowiska wirtualnego (Disaster Recovery)

4. Oprogramowanie musi współpracować z systemem wirtualizacyjnym Proxmox VE 8 które pracuje w WC, m.in. poprzez wykorzystywanie snap-shotów wykonywanych przez ten system.
5. Oprogramowanie musi mieć możliwość odtworzenia poszczególnych serwerów wirtualnych, kontenerów i fizycznych hostów w sposób zapewniający spójność danych.
6. Możliwość odtworzenie pojedynczych plików w obrębie serwera wirtualnego, kontenera.
7. Oprogramowanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji, w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
8. Oprogramowanie w przypadku konieczności instalacji wewnątrz maszyny wirtualnej agentów wymagających wdrożenia powinno być kompletne, czyli dostarczone z agentami dla następujących najnowszych wersji systemów operacyjnych i silników bazodanowych: Windows Serwer lic. 7, Linux RedHat lic. 2, Linux Debian lic. 4, MS SQL Serwer lic.7, Firebird lic.4, PostgresSQL lic 3
9. Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
10. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
11. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
12. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
13. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny.
14. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn z dowolnego backupu w izolowanym środowisku.
15. Licencje
    a. Dostarczone licencje muszą umożliwiać wykonywanie kopii zapasowych ze wszystkich serwerów fizycznych będących częścią Węzła Centralnego serwerów fizycznych zakupionych w ramach Środowiska Testowego
    b. Licencja musi umożliwiać wykorzystanie wszystkich opisanych w niniejszym dokumencie funkcjonalności, bez konieczności dokupowania jakichkolwiek dodatkowych opcji.
    c. Licencja nie może posiadać żadnego ograniczenia czasowego ani jeśli chodzi o ważność licencji, ani jeśli chodzi o termin użytkowania oprogramowania.
    d. W sytuacji, gdy oprogramowanie do archiwizacji danych wymaga do poprawnego działania jakiegoś dodatkowego, licencjonowanego oprogramowania (np. systemu operacyjnego), to Wykonawca musi dostarczyć te licencje wraz z oprogramowaniem do archiwizacji danych.
16. Aktualizacja 12 miesięcy

5.4 Urządzenie macierzowe do replikacji kopii zapasowej z SOKZ

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 zatokami na dyski SATA HDD i SSD o wielkości 3,5 cala oraz 2,5 cala.
2. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack.
3. Zainstalowany 1 procesor klasy x86 min. 4-rdzeniowy o taktowaniu min. 2.2GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 5400 pkt. Wynik należy dołączyć do oferty.
4. Pamięć RAM min. 32 GB RAM DDR4.
5. Wbudowane porty min. 2 porty USB 3.2

6. Powyższe porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
7. Min. 1 aktywny slot PCI-E 3.0 x8 umożliwiający instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe, karty SSD NVMe lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
8. Zainstalowane i w pełni funkcjonalne minimum 4 porty 1GbE RJ45. Porty nie mogą zajmować slotów PCI-E
9. Zainstalowane i w pełni funkcjonalne minimum 2 porty 10GbE SFP+ z modułami optycznymi MM.
10. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10.
11. Pamięć masowa:
    a. Zainstalowane min. 2 dyski SSD o pojemności min. 960 GB każdy.
    b. Zainstalowane min. 4 dyski HDD SATA o pojemności min. 8 TB każdy.
12. Min. 2 wentylatory.
13. Min. 2 zasilacze o mocy min. 350W, zainstalowane wewnątrz serwera, pracujące redundantni w celu zapewnienia ciągłości pracy w przypadku awarii jednego z nich.
14. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie AES-NI.
15. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków i zasilaniu.
16. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia kopii zapasowych i odzyskiwania danych komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
    a. Zaawansowane funkcje tworzenia kopii zapasowych
    b. Ochrona integralności danych oraz infrastruktury IT
    c. Natychmiastowe odzyskiwanie po awarii
    d. Deduplikacja
    e. Szyfrowanie i kompresja
    f. Statystyki użycia
    g. Wstrzymywanie i wznawianie tworzenia kopii zapasowych
17. Zgodność z normą ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami i 14001 lub równoważny spełniający wymagania związane z zarządzaniem środowiskowym, zgodnością z przepisami, ciągłym doskonaleniem na rzecz ochrony środowiska, monitorowaniem wpływu na środowisko.
26. Serwer musi posiadać deklaracja CE lub równoważne potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym.
18. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych.
19. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
20. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
21. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji.
22. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta w języku polskim.
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji.

c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
d. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami.
e. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
   i. możliwość pobierania najnowszego firmware,
   ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
   iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,

5.5 Zakres prac wdrożeniowych:

2. Analiza przedwdrożeniowa:
   a. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
   b. Opracowanie planu wdrożenia.
3. Wdrożenie i konfiguracja:
   a. Instalacja przełącznika oraz zestawienie połączenia z WC.
   b. Konfiguracja przełącznika zgodnie z wymaganiami zamawiającego.
   c. Instalacja i konfiguracja OKZ (Zainstalowanie na serwerze systemu do kopii zapasowej, konfiguracja puli magazynowych, konfiguracja interfejsów zarządzających w wydzielonej sieci MGMT)
   d. Konfiguracja zabezpieczeń.
   e. Integracja z istniejącymi systemami IT zamawiającego.
   f. Konfiguracja harmonogramu wykonywania kopii zapasowej, konfiguracja urządzenia macierzowego.
   g. Weryfikacja poprawności wykonania kopi zapasowej WC.
   h. Replikacja kopii zapasowych ma urządzenie macierzowe.
   i. Po instalacji ŚT przywrócenie w nim wybranego przez Zamawiającego jednego systemu z systemu kopi zapasowej oraz przywrócenie innego systemu wskazanego przez Zamawiającego z puli magazynowej replikowanej na urządzenie macierzowe.
4. Testy akceptacyjne:
   a. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
   b. Weryfikacja poprawności działania serwera wraz z oprogramowaniem.

6 Lokalizacja 2 – Środowisko Testowe (ŚT)

Zbudowanie Środowiska Testowego jest kolejnym etapem wzmacniania odporności Zamawiającego na zagrożenia. Głównym celem stawianym przed ŚT to odzwierciedlenie środowiska produkcyjnego WC zrealizowanego w ramach grantu Cyfrowa Gmina.
ŚT będzie miało główne cechy systemu produkcyjnego, nie będzie miało jego wydajności. Natomiast wyspecyfikowane rozwiązanie w ramach prowadzenia następujących prac: wykonania poprawności kopii, aktualizacji systemów, zmiana konfiguracyjnych będzie wystarczające. Ponadto w przypadku

katastrofalnej awarii WC będzie mogło przejąć rolę rozwiązania produkcyjnego dla systemów krytycznych Zamawiającego.

1. Budowa Środowiska Testowego:
   1.1. ŚT ma być utworzenie z 2 serwerów fizycznych jako zduplikowanego środowiska pracującego w trybie active-active (umowne nazwy dla serwerów: „pvet1", „pvet2").
   1.2. Każdy z serwerów będzie wykorzystywało własne zasoby dyskowe.
   1.3. Na każdym z serwerów zostanie zainstalowane oprogramowanie do wirtualizacji.
   1.4. Oprogramowanie do wirtualizacji będzie miało funkcjonalność, umożliwiającą replikację wybranych zasobów dyskowych z jednego serwera fizycznego do drugiego.
   1.5. Jako system wirtualny zostanie zainstalowany Serwerowego Systemu Operacyjnego do stworzenia serwera usług katalogowych.
2. Wymagane usługi instalacyjno-wdrożeniowe
   2.1. W ramach budowy Środowiska Testowego Wykonawca dostarczy i zainstalował opisany w tym rozdziale sprzęt do Lokalizacji 2.
   2.2. Skonfiguruje port do zdalnego zarządzania serwerem dla każdego z zakupionych serwerów.
   2.3. Zainstaluje i skonfiguruje oprogramowanie do wirtualizacji dla „pvet1" i „pvet2". Przed rozpoczęciem prac Wykonawca ustali z Zamawiającym sposób bootowania serwerów (czy z macierzy dyskowej, czy z pamięci SSD znajdującej się w każdym z serwerów);
   2.4. Zainstaluje i skonfiguruje w środowisku wirtualnym w „pvet1", oprogramowanie do obsługi usług katalogowych.
   2.5. Uruchomi replikację serwera wirtualnego na serwer pvet2.
   2.6. Założy i skonfiguruje w usłudze katalogowej konto dla przykładowego użytkownika.
   2.7. Będąc zalogowany do SSO z poziomu wirtualizatora zostanie wydane polecenie migracji maszyny wirtualnej na serwer przeciwstawny. Dopuszczalne jest kilkunastosekundowe zmrożenie konta zalogowanego do SSO. Gdzie po zakończeniu migracji system ma być w pełni sprawny.
3. Wykonanie punktów pkt. 2.1 do pkt. 2.7 będzie wymogiem podpisania protokół odbioru przedmiotu umowy.

6.1 Specyfikacja serwerów wchodzących w skład Środowiska Testowego

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 2 szt. serwerów pracujących w klastrze HA przeznaczonych do symulacji środowiska wirtualizacji i instalacji SSO realizujące usługi katalogowe.

1. Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji min. 8 dysków 2,5". Serwer musi posiadać możliwość rozbudowy o 2 dodatkowe wnęki dyskowe na dyski SAS/SATA/NVMe 2.5".
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz wyposażeniem w przedni panel zamykany na klucz, chroniącym dyski przed nieuprawnionym wyjęciem.
3. Płyta główna z możliwością zainstalowania do dwóch procesorów.
4. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5. Zainstalowany procesor min. 12-rdzeniowy o taktowaniu min. 2.4GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów min. 380 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 128 GB RAM DDR5 RDIMM 5600MT/s.
7. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
8. Zabezpieczenie pamięci:
   8.1. Memory mirroring
   8.2. ECC
   8.3. patrol scrubbing

8.4. SDDC
8.5. memory thermal throttling
8.6. ADDDC-SR
8.7. PPR
8.8. Memory SMBus hang recovery.

9. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
10. Wbudowane porty:
    10.1. min. 4 porty USB z czego nie mniej niż 1 x USB 3.0 na przednim panelu obudowy, 2 x USB 3.0 na tylnym panelu obudowy oraz 1 x USB 2.0 na płycie głównej;
    10.2. dodatkowo złącze USB TYP-C na przednim panelu, które musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS;
    10.3. port VGA na tylnym panelu obudowy;
    10.4. powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
11. Minimum 2 aktywne sloty PCI-E 5.0 x16.
12. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    12.1. minimum 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ Multimode
    12.2. minimum 4 porty 1Gb/s Ethernet w standardzie Base-T
13. Pamięć masowa:
    13.1. zainstalowane 2 dyski serwerowe SSD M.2 Read-Intensive Hot-Plug o pojemności min. 480 GB każdy. Dyski muszą być skonfigurowane w RAID1 przez dedykowany kontroler sprzętowy i nie mogą zajmować kieszeni na dyski 3.5”.
    13.2. zainstalowane 4 dyski serwerowe NVMe o pojemności min. 960 GB każdy.
14. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
15. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
16. Min. dwa identyczne zasilacze o mocy min. 1600W klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera. W komplecie z zasilaczami należy dostarczyć kable zasilające o długości min. 2m.
17. Bezpieczeństwo:
    17.1. wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    17.2. moduł TPM 2.0.
18. Możliwość wyposażenia serwera w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:
    18.1. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS
    18.2. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy
    18.3. przywracanie konta administratora
    18.4. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera
    18.5. wyświetlanie w czasie rzeczywistym temperatury procesorów
    18.6. konfigurowanie ustawień sieciowych modułu zarządzania.
19. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:
    19.1. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),
    19.2. monitorowanie w czasie rzeczywistym poboru prądu przez serwer,
    19.3. zbieranie logów błędów hardware,

19.4. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,
19.5. montowanie wirtualnych napędów,
19.6. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,
19.7. wysyłanie zawiadomień droga mailową i poprzez SNMP
19.8. wsparcia dla IPMI, SSH, Redfish
19.9. wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,
19.10. nadawanie ról użytkownikom,
19.11. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,
19.12. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.

20. Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    20.1. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.
    20.2. tworzenie szablonów instalacyjnych dla systemów operacyjnych.
    20.3. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.
    20.4. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.
    20.5. aktualizacja sterowników i BIOS serwerów.
    20.6. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
21. Zgodność z normami:
    - ISO 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami
    - ISO 14001 lub równoważny spełniający wymagania związane z zarządzaniem środowiskowym, zgodnością z przepisami, ciągłym doskonaleniem na rzecz ochrony środowiska, monitorowaniem wpływu na środowisko
    - ISO 27001 lub równoważny spełniający wymagania dotyczące zarządzania bezpieczeństwem informacji, ochrony danych i zarządzania ryzykiem
    - ISO 50001 lub równoważny zapewniający zarządzanie efektywnością energetyczną, ciągłe doskonalenie procesów energetycznych i zgodność z przepisami prawnymi dotyczącymi ochrony środowiska
22. Serwer musi posiadać deklarację CE lub równoważny potwierdzający dopuszczenie sprzętu do obrotu w Europejskim Obszarze Gospodarczym.
23. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
24. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
25. Gwarancja
    25.1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta w języku polskim.
    25.2. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day godziny od momentu zgłoszenia usterki.

25.3. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
25.4. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.
25.5. Usługi gwarancyjne świadczone przez producenta lub autoryzowanego partnera serwisowego producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny zapewniający zarządzanie jakością, podejście procesowe, ciągłe doskonalenie, zarządzanie ryzykiem oraz zgodność z przepisami.
25.6. Wymaganie oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
25.7. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
a. możliwość pobierania najnowszego firmware,
b. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
c. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
d. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

6.2 Oprogramowanie do wirtualizacji

1. Razem z serwerem należy dostarczyć oprogramowanie do wirtualizacji (np. Proxmox VE 8) uprawniające do uruchomienia dowolnej ilości serwerów wirtualnych oraz nie posiadające żadnego ograniczenia czasowego ani jeśli chodzi o ważność licencji, ani jeśli chodzi o termin użytkowania oprogramowania o poniższych wymaganiach (ilość licencji powinna pokrywać cały klaster HA złożony z 2 serwerów):
1.1. System musi być zainstalowany bezpośrednio na sprzęcie fizycznym, bez konieczności instalacji dodatkowego systemu operacyjnego.
1.2. System musi umożliwić uruchomienie wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Przy czym wspierane muszą być przynajmniej następujące systemy operacyjne:
a. Windows Server w wersji co najmniej 2019, 2022 i 2025.
b. Suse Linux Enterprise Server w wersji 10 i nowszej,
c. Red Hat Enterprise Linux w wersji 5 i nowszej.
1.3. System musi umożliwiać zastosowanie w serwerach fizycznych, procesorów o dowolnej ilości rdzeni oraz zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
1.4. System musi umożliwiać przydzielenie maszynom wirtualnym, łącznie większej przestrzeni dyskowej niż jest fizycznie dostępna w zasobach dyskowych.
1.5. System musi posiadać możliwość sprzętowego wsparcia dla wirtualizacji zagnieżdżonej.
1.6. System musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami, w tym możliwość monitorowania wykorzystania zasobów fizycznych, infrastruktury wirtualnej.
1.7. Konsola do zarządzania środowiskiem wirtualnym musi pochodzić od tego samego producenta co sam system do wirtualizacji, tak aby Zamawiający nie był zmuszony do szkolenia pracowników u dwóch różnych (lub więcej) producentów. Awaria pojedynczego serwera nie może blokować dostępu do konsoli zarządzania.

1.8. Dostęp przez przeglądarkę do graficznej konsoli zarządzania musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji, w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
1.9. System musi zapewniać możliwość wykonywania kopii migawkowych serwerów wirtualnych i instancji systemów operacyjnych, na potrzeby tworzenia kopii zapasowych (bez przerywania pracy tych systemów i serwerów wirtualnych).
1.10. System musi umożliwiać tworzenie replik obrazów dyskowych maszyn wirtualnych. System musi umożliwiać określenia częstotliwości wykonywania ww. kopii zasobów dyskowych.
1.11. System musi umożliwiać tworzenie klastrów z serwerów fizycznych, w celu zapewnienia wysokiej dostępności maszyn wirtualnych i aplikacji (high availability).
1.12. System musi posiadać możliwość przydzielania i konfiguracji uprawnień użytkownikom poprzez integrację z usługami katalogowymi (np. Microsoft Active Directory. LDAP itp.).
1.13. System musi pozwalać na tworzenie wirtualnych przełączników LAN, obsługę sieci vLAN.
1.14. System musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
1.15. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
1.16. Kopie zapasowe muszą być składowane z wykorzystaniem technik deduplikacji danych.
1.17. Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione, bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
1.18. Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku awarii tego repozytorium.
1.19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
1.20. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji.
1.21. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie przez system, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
1.22. Dla każdego środowiska wirtualnego wymagane jest oprogramowanie pochodzące od tego samego producenta co sam system do wirtualizacji, które w przypadku poważnej awarii (katastrofy) jednego z centrów danych, zautomatyzuje i przyspieszy uruchomienie krytycznych systemów użytkownych w drugim środowisku. Oprogramowanie to:
    a. Będzie wykorzystywało repliki (kopie) obrazów dyskowych, wykonywanych przez system do wirtualizacji;
    b. Umożliwi tworzenie grup serwerów wirtualnych, które powinny być odtwarzane razem (np. dla systemu obiegu dokumentów: serwer bazodanowy, serwer aplikacyjny i serwer WWW);
    c. Umożliwi przygotowanie skryptów, określających w jakiej kolejności, jakie zasoby należy zwolnić w lokalizacji zapasowej (np. wyłączyć pewne serwery wirtualne) i jakie uruchomić z kopii, aby przywrócić do pracy najbardziej krytyczne systemy użytkowe;

d. Umożliwi przygotowywanie ww. skryptów w tej samej konsoli zarządzającej, co cały system do wirtualizacji;

1.23. Aktualizacja 12 miesięcy

6.3 Oprogramowanie do realizacji Usług Katalogowych

1. Razem z serwerem należy dostarczyć Windows Server 2022 Standard (ilość licencji umożliwiającą bezproblemową pracę Systemowi Usług Katalogowych w Klastrze wysokiej dostępności złożony z 2 kupowanych serwerów) oraz umożliwić zarządzanie poprzez usługę katalogową min. 5 urządzeń (urządzenia, które będą wykorzystywane do testowanie zmian polityk bezpieczeństwa). Opis równoważności licencji oprogramowania:
   1.1. Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory, które jest aktualnie wykorzystywane. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerach zakupionym w ramach niniejszego postępowania tworzących klaster HA.
   1.2. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
   1.3. Licencja bez ograniczeń czasowych.
   1.4. Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
   1.5. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
   1.6. Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
   1.7. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;
   1.8. Praca w roli klienta domeny Microsoft Active Directory;
   1.9. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
   1.10. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
   1.11. Zawarta możliwość uruchomienia roli serwera DNS;
   1.12. Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
   1.13. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
   1.14. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
   1.15. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
   1.16. Zawarta możliwość uruchomienia roli serwera stron WWW;
   1.17. Zawarta funkcjonalność szyfrowania dysków;
   1.18. Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
   1.19. W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;
   1.20. W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
   1.21. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

1.22. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
1.23. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
1.24. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
1.25. Obsługa zdalnego pulpitu;
1.26. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
1.27. Obsługa PowerShell 4.0;

6.4 Zakres prac wdrożeniowych

1. Analiza przedwdrożeniowa:
    a. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
    b. Opracowanie planu wdrożenia.
2. Wdrożenie i konfiguracja:
    a. Instalacja serwera wraz z oprogramowaniem.
    b. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
    c. Integracja ŚT z OKZ
    d. Integracja z istniejącymi systemami IT zamawiającego.
3. Testy akceptacyjne:
    a. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
    b. Weryfikacja poprawności działania serwera oraz oprogramowania.