Spis treści

Kryteria ogólne 2

Kwalifikacje techniczne Wykonawców 3

**Kryterium oceny oferty………………………………………………………… 4**

**Do formularza ofertowego 6**

**Klaster UTM 7**

**Macierz dyskowa…………………………………………………… 14**

**Serwery RACK…………………………………………………………………………………… 23**

[**System operacyjny 29**](#_Toc158060721)

**Akcesoria sieciowe 34**

**Wdrożenie 35**

**Szkolenie 36**

1. **Kryteria ogólne:**
   1. Przedmiotem zamówienia jest dostawa serwerów, macierzy, urządzeń typu UTM i oprogramowania systemowego oraz świadczenie usług wdrożenia i szkolenia.
   2. Na przedmiot zamówienia składa się w szczególności dostawa:
2. Klaster urządzeń typu UTM – 1 zestaw
3. Macierz dyskowa – 1szt.
4. Serwer RACK - 3 szt.
5. Oprogramowanie systemowe – 6 sztuk,
6. Wdrożenie – 1 zestaw
7. Szkolenie – 2 osoby
   1. Urządzenia, o których mowa powyżej muszą być:
8. Fabrycznie nowe, to znaczy wyprodukowane nie wcześniej niż we wrześniu 2023r. i z zachowaniem najwyższej jakości, a ponadto zgodne z wszelkimi wymogami Zamawiającego, wolne od wad technicznych i prawnych i objęte gwarancją jakości producenta;
9. Nieużywane, nie mogą być przedmiotem wystaw, bądź prezentacji, nie mogą być wcześniej wykorzystywane przez innego użytkownika;
10. Kompletne i nadające się do użytkowania zgodnie z ich funkcją i przeznaczeniem, niezwłocznie po ich dostarczeniu, gotowe do użytku bez żadnych dodatkowych zakupów, a także osoby trzecie nie mogą mieć w stosunku do nich żadnych praw i nie mogą być przedmiotem żadnego postępowania ani zabezpieczenia;
11. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 – przed podpisaniem umowy Zamawiający będzie wymagał przedłożenia stosownego certyfikatu odnoszącego się do całości produktu.
12. Serwer musi posiadać deklaracja CE – przed podpisaniem umowy Zamawiający będzie wymagał przedłożenia stosownej deklaracji
13. Macierz musi posiadać deklaracja CE – przed podpisaniem umowy Zamawiający będzie wymagał przedłożenia stosownej deklaracji
14. **Kwalifikacje techniczne wykonawców**

Wykonawca musi wykazać, że dysponuje osobami posiadającymi odpowiedne kwalifikacje do wykonania zamówienia.

* 1. Co najmniej jedną osobą posiadająca ważny certyfikat wystawiony przez producenta oferowaneg rozwiązania pamięci masowych (macierze) na poziomie minimum specjalisty/inżyniera, potwierdzający umiejętności z instalacji, konfiguracji, zarządzania i optymalizacji (deployment),
  2. Minimum jedna osoba posiadająca ważny certyfikat wystawiony przez producenta oferowanych serwerów na poziomie minimum specjalisty, potwierdzający umiejętności z instalacji, konfiguracji i rozwiązywania problemów (serwery)
  3. Minimum 1 kierownik projektu posiadający:

1. Kierownik projektu - osoba posiadająca kwalifikacje zarządzania projektami potwierdzone ważnym certyfikatem metodyki PRINCE2 na poziomie Practitioner lub równoważnym oraz posiadająca minimum 5 letnie doświadczenie w prowadzeniu projektów IT potwierdzonego min. 2 referencjami,

2) Doświadczenie w co najmniej 3 wdrożeniach systemu informatycznego na stanowisku kierownika   
 wdrożenia /projektu.

* 1. Zespół wdrożeniowy - co najmniej 2 specjalistów posiadających co najmniej 3 letnie doświadczenie w zakresie wdrożeniach systemów informatycznych.

1. **Kryteria oceny ofert**

**Cena – waga 60%**

**Parametry techniczne – waga 40%**

|  |  |  |  |
| --- | --- | --- | --- |
| **lp.** | **Parametry techniczne** | **Liczba Punktów** | **Spełnia**  **Tak/Nie** |
| 1 | **Macierz dyskowa**  Pamięć Write Cache jest mirrorowana (odpowiednik RAID1) nawet w razie awarii jednego z kontrolaów macierzy. | 10 |  |
| 2 | **Serwer RACK**  Wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą.  Zintegrowany z płytą główną moduł TPM 2.0.  Musi posiadać funkcjonalność UEFI Secure Boot, w zakresie minimum weryfikacji sygnatur kryptograficznych sterowników UEFI oraz kodu uruchamianego przed uruchomieniem systemu operacyjnego serwera.  Musi posiadać wsparcie dla trybu blokady, polegającego na zapobieganiu przed wprowadzaniem modyfikacji i aktualizacji ustawień konfiguracji oraz oprogramowania wewnętrznego serwera. | 10 |  |
| 3 | **Serwer RACK oraz Macierz Dyskowa**  serwisowana przez jednego producenta posiadającego jeden punkt zgłaszania awarii. | 10 |  |
| 4. | **UTM:**  Musi posiadać system blokowania i odpowiedzi na zaawansowane zagrożenia typu malware i ransomware o parametrach:  - musi posiadać agentów dedykowanych dla systemów operacyjnych co najmniej Windows 7, 8, 8.1, 10, 11, Windows Server 2008, 2012, 2016, 2019 Linux RedHat/CentOS, Mac OS 10.x,  - musi zostać dostarczone z licencja na wsparcie minimum 75 hostów (stacji roboczych i serwerów),  - musi posiadać możliwość prowadzenia analizy heurystycznej i behawioralnej pod kątem zagrożeń typu malware i ransomware, bezpośrednio na hostach i w trybie ciągłym wysyłać wyniki analizy do systemu centralnego w celu przeprowadzenia oceny zagrożeń dzięki korelacji i scoringu zagrożeń,  - musi posiadać mechanizm automatycznej odpowiedzi na wykryte zagrożenie typu malware i ransomware, poprzez minimum takie działania jak, kwarantanna plików, zabijanie procesów (ang. kill) i usuwanie wpisów w rejestrach,  - musi pozwalać na konfigurowalne powiadamianie poprzez e-mail minimum o wykrytych krytycznych zdarzeniach, incydentach, oraz akcjach podjętych aby im zapobiec które miały miejsce w sieci i na hostach. | 10 |  |

# **Do formularza ofertowego**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Pozycja oferty** | **Producent** | **Nazwa, model i wersja produktu lub oprogramowania** | **Liczba** | **Cena jednostkowa brutto w PLN** | **Wartość brutto** |
| 1 | Urządzenie UTM - klaster |  |  | 1 kpl. |  |  |
| 2 | Macierz dyskowa |  |  | 1 kpl. |  |  |
| 3 | Serwer RACK |  |  | 3 szt. |  |  |
| 4 | System operacyjny |  |  | 6 szt. |  |  |
| 5 | Akcesoria Sieciowe |  |  | 1 kpl. |  |  |
| 6 | Wdrożenie |  |  | 1 kpl. |  |  |
| 7 | Szkolenie |  |  | 1 kpl. |  |  |
| Suma Brutto | | | | | |  |

# **1x Klaster UTM**

Zamawiający wymaga dostarczenia klastra wysokiej dostępności urządzeń UTM działających minimum w trybie aktywny-pasywny (Active-Passive), w związku z czym każdy z węzłów klastra pełniąc rolę jako aktywny węzeł, musi spełniać poniższe wymagania.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L.p.** | | **Parametr** | **Charakterystyka (wymagania minimalne)** | | **Spełnia**  **TAK/NIE** |
| Nazwa i model proponowanego rozwiązania:  …………………………………………………………………………………………………………………………………………………………………………………. | | | | | |
| 1. | **Funkcjonalność Firewall** | | Firewall musi umożliwiać zdefiniowanie co najmniej 3 stref bezpieczeństwa |  | |
| Firewall musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP |  | |
| Firewall musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie |  | |
| Firewall musi obsługiwać DHPC v6 na zewnętrznym interfejsie |  | |
| Firewall musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach. |  | |
| Firewall musi mieć możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu i dynamiczną selekcją drogi routowania. |  | |
| Firewall musi mieć możliwość obsługi łącza zapasowego typu LTE |  | |
| Firewall musi obsługiwać Dynamic DNS |  | |
| Firewall musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1 |  | |
| Firewall musi obsługiwać translację portów: PAT |  | |
| Firewall musi obsługiwać IPSec NAT traversal |  | |
| Firewall musi obsługiwać mechanizm policy-based NAT |  | |
| Firewall musi obsługiwać VLAN 802.1Q |  | |
| Firewall musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów |  | |
| Firewall musi obsługiwać pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych. |  | |
| Firewall musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP |  | |
| Firewall musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego. |  | |
| Firewall musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników. |  | |
| Firewall musi umożliwiać transparentne uwierzytelnianie użytkowników przez Active Directory. |  | |
| Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp |  | |
| Urządzenie nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej. |  | |
| Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji |  | |
| Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen. |  | |
| Firewall musi obsługiwać mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów. |  | |
| Firewall musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP |  | |
| Firewall musi zapewniać ochronę z wykorzystaniem mechanizmów IPS |  | |
| Firewall musi zapewniać ochronę antywirusową dla obsługiwanych protokołów |  | |
| Firewall musi zapewniać możliwość filtrowania URL |  | |
| Firewall musi zapewniać inspekcję ruchu szyfrowanego HTTPS |  | |
| Firewall musi zapewniać ochronę przed niechcianą pocztą (AntySPAM) |  | |
| Firewall musi zapewniać rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu. |  | |
| Urządzenie musi mieć możliwość filtrowania treści według typu MIME |  | |
| Urządzenie musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji. |  | |
| Firewall musi udostępniać mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych. |  | |
| Firewall musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site |  | |
| Firewall musi posiadać mechanizm blokujący szkodliwe żądania DNS, zapewniając ochronę użytkowników końcowych przed atakami typu phishing |  | |
| 2. | **Wydajność firewall** | | Firewall musi zapewnić obsługę na poziomie minimalnym:  **17Gbps** dla pracy w trybie firewall (UDP 1518),  **2.2Gbps** dla pracy w trybie UTM |  | |
| Firewall musi obsługiwać minimum **4 400 000** jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną **95 000** nowych połączeń na sekundę. |  | |
| Ilość obsługiwanych sieci VLAN: minimum **200.** |  | |
| Minimalna ilość fizycznych portów:  - 8 portów 1Gbps RJ45  - 2 porty 10Gbps SFP+ |  | |
| 3. | **Funkcje VPN** | | Urządzenie musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS |  | |
| Urządzenie musi w zakresie IPSec site-to-site VPN współpracować z rozwiązaniami innych producentów |  | |
| Rozwiązanie musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256 |  | |
| Rozwiązanie musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert. |  | |
| Wsparcie dla Dead Peer Detection (DPD) |  | |
| Urządzenie musi obsługiwać IKEv1 i IKEv2 |  | |
| Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web |  | |
| Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP |  | |
| Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu |  | |
| Urządzenie musi obsługiwać statyczne i dynamiczne (routowane) połączenia VPN do dostawców chmury obliczeniowej (AWS i MS Azure) |  | |
| Urządzenie musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP. |  | |
| Połączenia client-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android |  | |
| Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu |  | |
| Urządzenie ma zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS) |  | |
| 4. | **Wydajność VPN** | | Przepustowość IPSec VPN (UDP 1518) nie mniejsza niż **5.0Gbps** |  | |
| Obsługa nie mniej niż: **200** tuneli IPSec site-to-site |  | |
| Obsługa nie mniej niż: **200** tuneli client-to-site |  | |
| 5. | **Filtrowanie zawartości URL** | | Urządzenie musi umożliwiać filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji |  | |
| Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według minimalnie 120 kategorii |  | |
| Rozwiązanie musi pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości |  | |
| Baza zawartości URL powinna być dostępna on-line lub do ściągnięcia i zainstalowania miejscowo |  | |
| Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim |  | |
| Filtrowanie musi obsługiwać również protokół https |  | |
| Urządzenie musi umożliwiać wyłączenie inspekcji https dla wybranych kategorii stron www |  | |
| System kategoryzacji stron musi posiadać kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware |  | |
| 6. | **Kontrola aplikacyjna** | | System kontroli aplikacyjnej musi rozpoznawać aplikacje oraz kategorie aplikacji |  | |
| Aplikacje muszą być rozpoznawana w oparciu o analizę ruchu a nie przez porty i protokoły |  | |
| Ilość rozpoznawanych aplikacji nie mniejsza niż 1800 |  | |
| W ramach konkretnej aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe) |  | |
| Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online |  | |
| 7. | **Antywirus** | | System musi mieć możliwość uruchomienia co najmniej 2 skanerów antywirusowych |  | |
| Aktualizacja plików sygnatur antywirusowych musi się odbywać automatycznie |  | |
| Aktualizacja plików sygnatur antywirusowych musi się odbywać nie rzadziej niż co 12 godzin. |  | |
| Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail. |  | |
| Jeden ze skanerów antywirusowych musi bazować na mechanizmach bezsygnaturowych |  | |
| Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen |  | |
| Wykrywanie i blokowanie spyware’u |  | |
| Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji |  | |
| Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS |  | |
| Przepustowość AV w urządzeniu nie mniejsza niż **3Gbps** |  | |
| W celu realizacji ochrony z wykorzystaniem 2 skanerów antywirusowych Zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia. |  | |
| 8. | **Antyspam** | | Antyspam ma zapewnić możliwość kwarantanny e-mail |  | |
| Antyspam ma posiadać zintegrowaną antywirusową analizę spamu |  | |
| Rozwiązanie ma umożliwić blokowanie spamu w wielu językach w tym w języku polskim |  | |
| Możliwość blokowania spamu opartego na obrazach graficznych. |  | |
| 9. | **IPS** | | Automatyczna aktualizacja sygnatur IPS |  | |
| IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy |  | |
| Automatyczne blokowanie znanych źródeł ataków |  | |
| System musi pozwalać na blokowanie ataków typu DoS i DDoS |  | |
| Przepustowość IPS w urządzeniu nie mniejsza niż **3.2Gbps** |  | |
| 10. | **WiFi** | | UTM musi mieć możliwość pełnienia funkcji kontrolera sieci WiFI. |  | |
| Kontroler sieci wifi ma zapewniać centralne zarządzanie oraz serowanie punktami dostępowymi. |  | |
| Sieć ma mieć możliwość jednoczesnej pracy w paśmie 2.4Ghz oraz 5Ghz. |  | |
| Sieć ma mieć możliwość skonfigurowania co najmniej 8 SSID w każdym z zakresów (2.4GHz i 5GHz) |  | |
| Sieć musi posiadać mechanizmy wykrywania innych punktów dostępu (ang. rogue access point) |  | |
| Sieć musi mieć możliwość izolacji urządzeń końcowych |  | |
| Sieć musi mieć możliwość uruchamiania poszczególnych SSID wg harmonogramu |  | |
| Musi istnieć możliwość automatycznej aktualizacji oprogramowania punktów dostępowych przez kontroler sieci WiFi |  | |
| Kontroler musi mieć funkcję graficznej prezentacji topologii sieci |  | |
| Kontroler musi mieć funkcję analizy mapy konfliktów w kanałach transmisyjnych |  | |
| Sieć musi obsługiwać minimum następujące mechanizmy bezpieczeństwa: WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK (Mixed), WPA-802.1X (Enterprise) WPA2-802.1X (Enterprise) WPA-802.1X/WPA2-802.1X (Mixed), TKIP, AES, TKIP/AES, Captive Portal, MAC whitelist/blacklist, VLAN Tagging |  | |
| 11. | **Ochrona przed phishingiem** | | System musi zapewniać dedykowaną (poza ochroną przed SPAMem) ochronę przed phishingiem |  | |
| System winien blokować możliwość dostępu do spreparowanych stron. |  | |
| System musi blokować dostęp niezależnie od użytego protokołu czy portu komunikacyjnego |  | |
| Zablokowanie dostępu musi być odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów |  | |
| System musi chronić przed nadużyciem protokołu DNS |  | |
| 12. | **Zarządzanie** | | Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym. |  | |
| Urządzenie musi umożliwiać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH. |  | |
| Urządzenie musi umożliwiać zarządzanie za pomocą wbudowanego interfejsu www. |  | |
| Interfejs WWW do zarządzania urządzeniem musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach. |  | |
| Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów. |  | |
| Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail. |  | |
| Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online |  | |
| System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia. |  | |
| Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji. |  | |
| System ma posiadać metodę porównywania różnych wersji konfiguracji. |  | |
| Obsługa różnych ról administratorów. |  | |
| Umożliwia monitorowanie logów ruchu w czasie rzeczywistym. |  | |
| System ma posiadać możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty) |  | |
| Urządzenie musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi. |  | |
| System zarządzania musi zapewniać korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów |  | |
| System zarządzania musi posiadać graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop |  | |
| 13. | **Dzienniki i raporty** | | Rozwiązanie musi umożliwiać zbieranie i przechowywanie dzienników i raportów. |  | |
| Rozwiązanie musi umożliwiać przesyłanie logów do co najmniej 2 serwerów dziennika |  | |
| Dzienniki transmisji muszą być szyfrowane. |  | |
| Rozwiązanie musi zapewniać narzędzie graficznej analizy logów. |  | |
| Rozwiązanie musi udostępniać narzędzie analizy całości ruchu |  | |
| Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa |  | |
| Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów czy rozmiaru bazy danych |  | |
| Rozwiązanie musi posiadać minimum 90 predefiniowanych typów raportów. |  | |
| Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie |  | |
| System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV. |  | |
| System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail. |  | |
| Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości. |  | |
| System raportowania musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników. |  | |
| System musi wspierać automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną. |  | |
| Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom. |  | |
| System musi umożliwiać pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów |  | |
| System musi zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu. |  | |
| 14. | **Zero Day / Zaawansowana Detekcja Malware** | | Funkcja zaawansowanego wykrywania szkodliwego oprogramowania w tym samym urządzeniu. |  | |
| Zaawansowany Malware jest wykrywany przez uruchomienie plików w chmurze przy użyciu emulacji pełnego systemu. |  | |
| Zaawansowana Detekcja Malware musi obsługiwać wszystkie pliki wykonywalne systemu Windows, pliki zip, pdf, Microsoft Office, oraz pliki Android APK. |  | |
| Wymagane są szczegółowe raporty, oraz informacje wskazujące na powody, dla których plik jest uważany za zaawansowany Malware |  | |
| W celu realizacji ochrony „Zero Day” zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia. |  | |
| 15. | **Konfiguracja rozwiązania, gwarancja, wdrożenie.** | | Okres wsparcia technicznego – minimum **3-lata**. |  | |
| Urządzenie musi być dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności wymienionymi w niniejszej specyfikacji. Długość trwania licencji/subskrypcji nie może być krótsza niż okres wsparcia technicznego. |  | |
| Możliwość zgłaszania incydentów za pomocą e-mail, portalu - 24 godziny na dobę 7 dni w tygodniu |  | |
| Zamawiający wymaga by wymiana urządzenia w przypadku zdiagnozowania awarii uniemożliwiającej funkcjonowanie, następowała na następny dzień roboczy od zdiagnozowania awarii (advanced hardware replacement NBD). |  | |

**6) 1x Macierz dyskowa**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Spełnia**  **TAK/NIE** |
| Nazwa i model proponowanego rozwiązania:  …………………………………………………………………………………………………………………………………………………………………………………. | | | |
|  | **Licencja** | Rozwiązanie musi być dostarczone z licencjami na wszystkie dostępne dla systemu funkcjonalności oraz dyski dla maksymalnej do uzyskania w oferowanym modelu pojemności RAW. |  |
|  | **Standard RACK** | Wymagane jest rozwiązanie mieszczące się w standardowej, pojedynczej szafie RACK 19”, Preferowane jest rozwiązanie kompaktowe tj. o jak najmniejszym rozmiarze fizycznym. |  |
|  | **Obsługa komunikacji do hosta** | Rozwiązanie musi być zbudowane w oparciu o dwa lub wielokrotność dwóch kontrolerów macierzowych obsługujących dane wejścia/wyjścia w trybie active-active.  Tryb pracy portów active-active jest wymagany dla każdej pary kontrolerów w macierzy. Niedopuszczalne są rozwiązania active-passive.  Macierz musi być wyposażona w procesory wyposażone we wsparcie dla protokołu NVMe (nie starsze niż Intel Skylake). Minimalna ilość core-ów dla każdego kontrolera – 20. Minimalna ilość pamięci RAM dla każdego kontrolera - 192GB. |  |
|  | **Pojemność** | Oferowana macierz musi składać się z minimum 10 dysków lub modułów flash nie mniejszych niż 3,2TB każdy.  Macierz w oferowanej konfiguracji musi zapewniać minimum 25TiB przestrzeni użytkowej oraz minimum 34TiB powierzchni RAW. Przestrzeń użytkowa nie może uwzględniać jakiejkolwiek redukcji danych w oparciu o machanizmy kompresji, deduplikacji itp.  Zapełnienie macierzy w 100% dostępnej pojemności nie może powodować utraty dostępu do danych.  Oferowany system musi w pełni być oparty o protokół NVMe tj wszelkie operacje wewnętrzne macierzy muszą być realizowane poprzez NVMe. Niedopuszczalny jest protokół SAS w żadnym elemencie rozwiązania, niezależnie od jego skali. |  |
|  | **Ochrona nośników danych** | Musi być realizowana za pomocą tzw. rozproszonej parzystości na poziomie blokowym. Niedopuszczalne są klasyczne realizacje ochrony danych oparte o grupy dysków w RAID 4/5/6 czyli niedopuszczalne jest stosowanie dedykowanych dysków parzystości tzw. parity drives oraz dedykowanych dysków zapasowych tzw. hot spare drives.  Niedopuszczalne jest stosowanie dysków dedykowanych tylko do konkretnych typów danych. |  |
|  | **Ochrona danych** | Rozwiązanie musi oferować mechanizm weryfikacji odczytywanych danych, wykrywania i naprawiania uszkodzonych danych w sposób przezroczysty dla hosta.  Rozwiązanie musi oferować mechanizm monitorowania trwałości nośników i realizować funkcję proaktywnej odbudowy, czyli zgłoszenia awarii nośnika.  Rozwiązanie musi być odporne na awarię co najmniej jednego dowolnego nośnika danych.  Rozwiązanie musi mieć możliwość skonfigurowania w taki sposób, aby być odporne na jednoczesną awarię minimum dwóch dowolnych nośników danych, niezależnie od skali i konfiguracji rozwiązania i w takim przypadku macierz musi zapewnić bezprzerwowy dostęp do wszystkich danych na macierzy.  Oferowany system dyskowy musi implementować funkcjonalność „software WORM” dla danych bądź kopii zapasowych danych - np. w postaci zabezpieczania danych / kopii migawkowych przed usunięciem – na minimum 30 dni. Jeśli do realizacji tej funkcjonalności wymagane jest oprogramowanie zewnętrzne musi zostać dostarczone wraz z niezbędną infrastrukturą do jej uruchomienia ora objąć licencją pełną pojemność macierzy. |  |
|  | **Bezpieczeństwo danych** | Rozwiązanie musi szyfrować wszystkie przechowywane dane minimum algorytmem AES-256 lub silniejszym oraz mieć możliwość szyfrowania wszystkich nośników obsługiwanych w urządzeniu.  Szyfrowanie danych nie może mieć wpływu na wydajność rozwiązania*.*  Klucz szyfrujący musi być przechowywany na macierzy i generowany w sposób uniemożliwiający odczyt danych z usuniętych z macierzy nośników. |  |
|  | **Rozbudowa przestrzeni dyskowej** | Rozbudowa pojemności rozwiązania musi być możliwa o zestaw nośników lub modułów Flash w celu zwiększenia elastyczności rozbudowy. Oferowany system musi rozbudowywać się do minimum 1PB powierzchni dyskowej RAW w ramach oferowanych kontrolerów.  Niedopuszczalne jest stosowanie dodatkowych kontrolerów macierzowych łączonych po FC lub RDMA.  Jeśli w ramach rozbudowy dołączana jest półka dyskowa musi być ona łączona poprzez protokół NVMe. |  |
|  | **Porty do transmisji danych** | Rozwiązanie musi posiadać natywne podłączenie do sieci SAN poprzez protokół Fibre Channel o minimalnej liczbie portów 8 i o minimalnej przepustowości każdego portu 32 Gbps, oraz oferować połączenia poprzez protokół iSCSI o minimalnej liczbie portów 8 i minimalnej przepustowości każdego portu 25Gb (SFP28)**.** Wymagane jest aby macierz posiadała możliwość rozbudowy o dodatkowe cztery interfejsy 100GbE w ramach oferowanych kontrolerów. Niedopuszczalne jest stosowanie sprzętu pośredniczącego iSCSI-FC itp. Wszystkie porty musza być obsadzone odpowiednimi modułami/wkładkami.  Niedopuszczalne jest wykorzystywanie portów FC do łączenia kontrolerów macierzowych.  Kontrolery muszą wspierać jednocześnie ruch - blokowy i plikowy (wymagane protokoły: iSCSI, FC oraz plikowy CIFS - minimum SMB w wersjach 1,2,3,3.11 FTP i SFTP oraz NFS). Nie dopuszcza się realizacji funkcjonalności ruchu plikowego za pomocą dodatkowych/zewnętrznych urządzeń.  Zastosowane karty oraz porty frontend muszą obsługiwać protokół NVMe-o-F (NVMe over Fabrics). Zmiana wykorzystywanego przez karty protokołu pomiędzy FC a NVMe-o-F musi być możliwa dla administratora oraz odbywać się bezprzerwowo z punktu widzenia dostępu do danych. |  |
|  | **Wysoka dostępność** | Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń.  Należy dostarczyć licencje do obsługi wszystkich wymienionych typów replikacji dla pełnej możliwej do uzyskania pojemności RAW oferowanych systemów.  Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem.  Rozwiązanie musi posiadać funkcjonalność replikacji synchronicznej umożliwiające utworzenie z macierzytej samej klasy,A klastra active-active (pomiędzy dwiema serwerowniami zlokalizowanymi w osobnych budynkach) oraz posiadać wszystkie komponenty sprzętowe niezbędne do realizacji funkcjonalności replikacji. Jeżeli takowe komponenty są używane ich właściwości - typu rozmiar fizyczny, zużycie energii - muszą zostać wliczone w całkowity rozmiar rozwiązania.  Replikacja synchroniczna musi być możliwa dla minimum jednego wolumenu (LUNa). Jakakolwiek zmiana ilości replikowanych wolumenów nie może wymagać zmiany konfiguracji sprzętowej macierzy.  Replikowany wolumen danych musi być dostępny do odczytu/zapisu w obu lokalizacjach jednocześnie.  W przypadku awarii sprzętowej w jednej lokalizacji rozwiązanie musi automatycznie przełączyć pełną funkcjonalność do drugiej lokalizacji. |  |
|  | **Niezawodność** | Rozwiązanie musi oferować dostępność na poziomie minimum 99,999% lub wyższym. Potwierdzenie realizacji tej funkcjonalności musi znajdować się w oficjalnej dokumentacji producenta oferowanego sprzętu.  Architektura rozwiązania nie może mieć pojedynczego punktu awarii (tzw. SPOF ang. „Single point of failure"). Musi istnieć możliwość wymiany komponentów na gorąco bez przerywania działania macierzy dyskowej w szczególności dotyczy to zasilaczy i wentylatorów Dane muszą być dostępne w przypadkach:  - awarii jednej linii zasilania,  - awarii dowolnego kontrolera,  - awarii dowolnych dwóch nośników danych użytkownika,  - awarii dowolnego portu FC/iSCSI,  - awarii dowolnego modułu pamięci RAM lub dowolnego procesora kontrolera.  Awaria i niedostępność pojedynczego kontrolera macierzy nie może powodować spadku wymaganej wydajności całego rozwiązania – brak efektu tzw. „Degraded Performance failover”. Oznacza to iż macierz musi posiadać wymaganą wydajność (w obydwu stanach: awarii oraz braku awarii.  Zmiana wersji oprogramowania zarządzającego rozwiązaniem lub oprogramowania wbudowanego w kontrolery rozwiązania nie może powodować utraty dostępu do danych.  Rozwiązanie musi umożliwiać wymianę na gorąco (bez zatrzymywania dostępu do danych) następujących komponentów: kontrolerów, zasilaczy, wentylatorów, portów front-end i back-end, nośników danych.  Rozwiązanie musi umożliwiać bezpieczne wyłączenie urządzenia niepowodujące utraty danych użytkownika. Dane przechowywane w pamięci urządzenia muszą zostać trwale zapisane na nośniki nieulotne przed całkowitym wyłączeniem macierzy na skutek awarii bądź interwencji manualnej. |  |
|  | **Zarządzanie** | Rozwiązanie musi udostępniać graficzną konsolę zarządzającą (GUI) poprzez interfejs Web (HTML5), która umożliwia monitorowanie stanu i obciążenia macierzy. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy.  Monitorowanie urządzenia musi być dostępne z w/w konsoli oraz obejmować swoim zakresem dane historyczne z okresu przynajmniej 1 roku wstecz.  Rozwiązanie musi umożliwiać monitorowanie:  - wykorzystania całkowitej pojemności fizycznej,  - wykorzystania pojemności logicznej,  - globalnego współczynnika redukcji danych - jeśli występuje  - wartości transferu danych (w MB/s) oraz ilości operacji (IOPS)  Rozwiązanie musi być zarządzane poprzez linię komend (CLI) dostępną poprzez protokół SSH. Dostęp do linii komend poprzez SSH musi być możliwy bez podawania hasła tj. przy wykorzystaniu kluczy uwierzytelniających.  Rozwiązanie musi udostępniać interfejs REST API oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi.  Rozwiązanie musi obsługiwać monitorowanie dla wydajności (Opóźnienie, IOPS, Odczyt/zapis, Szerokość pasma, Rozmiar IO, Długość kolejki), Pojemność (Łącznie, Oszczędność – redukcja danych, Snapshoty) i Konfiguracja z możliwością przekierowania powiadomienia na adres e-mail i łatwy dostęp poprzez aplikacje dostawców dla urządzeń mobilnych (Android i iOS). Rozwiązanie musi być hostowane w środowisku producenta macierzy i być udostępnione bez dodatkowych kosztów przez cały okres użytkowania proponowanego rozwiązania i zapewniać co najmniej 1 rok danych historycznych.  Macierz musi mieć wbudowane procedury pełnej i automatycznej diagnostyki elementów oraz możliwość natychmiastowego raportowania błędów do administratorów oraz do centrum wsparcia technicznego producenta w trybie 24/7/365. |  |
|  | **Funkcje prezentacji danych** | Rozwiązanie musi realizować funkcję thin-provisioningu dla wszystkich udostępnianych wolumenów (tzn. musi posiadać wbudowaną funkcjonalność umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.) oraz dostarczenie funkcji space reclamation tzn. rozwiązanie musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny i inicjowany bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych. |  |
|  | **Wbudowane funkcje macierzy** | Rozwiązanie musi oferować funkcję tworzenia natychmiastowych kopii wolumenów oraz oferować możliwość utworzenia przynajmniej 512 kopii wolumenu.  Rozwiązanie musi zapewniać hierarchiczne tworzenie kopii (np. kopia z kopii z kopii) wolumenów.  W momencie utworzenia kopia nie może zajmować dodatkowej przestrzeni dyskowej dostępnej dla użytkownika.  Rozwiązanie musi oferować możliwość natychmiastowego odtworzenia wolumenu z dowolnej kopii utworzonej z tego wolumenu bądź znajdującej się w dowolnym miejscu hierarchii kopii tego wolumenu. Odtworzony wolumen musi być natychmiast dostępny dla hosta w trybie read/write.  Rozwiązanie musi oferować możliwość natychmiastowego odświeżenia dowolnej kopii z dowolnej innej kopii lub wolumenu w ramach jego hierarchii. Odtworzona kopia musi być natychmiast dostępna dla hosta w trybie read/write.  Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie wielu wolumenów naraz tj tworzenie kopii zapasowej wielu LUNów w tej samej milisekundzie. Musi istnieć możliwość utworzenia wielu kopii naraz bez wykorzystania dodatkowej przestrzeni na macierzy.  Rozwiązanie musi zapewniać mechanizm kompresji i deduplikacji danych w trybie in-line. Kompresja i deduplikacja muszą być integralną częścią systemu macierzowego bez możliwości zatrzymania bądź wyłączenia przez administratora. Mechanizmy kompresji i dedpuplikacji muszą być przezroczysty dla administratora macierzy.  Wobec powyższych wymagań dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne dla wszystkich rodzajów przechowywanych danych (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności).  System operacyjny macierzy musi umożliwiać tworzenie spójnych kopii całych baz danych bądź aplikacji za pomocą zewnętrznego oprogramowania.  Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji w minimum wersjach:  a) Exchange 2016 i 2019, SQL Server 2017 i 2019, Oracle 18 i 19, VMware dla blokowych i plikowych datastore.  b) Spójność kopii rozumieć należy jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych.  c) Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. |  |
|  | **Skalowanie rozwiązania** | Macierz musi umożliwiać skalowalność wertykalną (scale-up) to jest taką, gdzie konfiguracja inicjalna zaczyna się od niepełnego obsadzenia dyskami i pozwala na instalowanie kolejnych dysków w wolnych slotach półki bez wpływu na dostępność do danych. Zamawiający dopuszcza rozwiązania skalowane horyzontalnie (scale-out) poprzez instalację dodatkowych kontrolerów. Wymagane jest, aby po takiej rozbudowie była możliwość zaprezentowania każdego wolumenu logicznego LUN przez dowolny z kontrolerów bez przerywania dostępu do danych.  Macierz musi posiadać (bez stosowania dodatkowych przełączników lub koncentratorów) możliwość skalowalności do minimum 16 portów Fibre Channel 32 Gbps lub 16 portów iSCSI 10 Gbps (jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów).  Macierz musi korzystać z globalnej puli nośników i danych niezależnie od wykorzystywanego kontrolera.  Rozwiązanie musi domyślnie wspierać pracę na wszystkich portach front-end w trybie round-robin w ramach danego kontrolera z niezmiennymi czasami odpowiedzi, niezależnie od aktualnie wykorzystywanego portu i wolumenu.  Niezależnie od rodzaju zapisanych danych i przy macierzy zapełnionej w przynajmniej 50% fizycznej pojemności, rozwiązanie w oferowanej konfiguracji musi oferować następującą wydajność na całej powierzchni dostępnej dla użytkownika, z aktywnymi i pracującymi wszelkimi oferowanymi funkcjami obsługi danych (optymalizacja, etc.)  - co najmniej 100 000 losowych operacji (70% odczytu, 30% zapisu, bez udziału cache macierzy) wykonywanych blokiem 8 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 1 ms,  Te same parametry wydajnościowe muszą być jednocześnie spełnione w przypadku, gdy w czasie testów trwających minimum 60 minut, na wolumenach poddanych obciążeniu:  - tworzone są kopie migawkowe  - dane są dodawane i usuwane |  |
|  | **Integracja** | Oferowany system dyskowy zapewnia wsparcie i kompatybilność z następującymi systemami operacyjnymi tj znajdować się na oficjalnej liście wsparcia poszczególnych producentów następującego oprogramowania:   * Vmware ESXi 6.7 i wyższe * MS Windows Server 2016 i wyższe * SLES 12 i wyższe * RHEL 7.5 i wyższe * Oracle Solaris 11 i wyższe * IBM AIX 7 i wyższe * HPE HP-UX 11 i wyższe   Oferowany system dyskowy musi znajdować się na aktualnej matrycy wsparcia Commvault Intellisnap.  https://documentation.commvault.com/snap/#/storage\_check  System operacyjny macierzy musi natywnie realizować funkcjonalność Vmware vVOLs oraz obsługiwać funkcjonalność Vmware VASA w wersji 3 wraz z Vmware VAAI, SRA, System musi udostępniać dedykowany plugin do vSphere Web Client umożliwiający zarządzanie macierzą poprzez interfejs Vmware vCenter.  System operacyjny macierzy musi umożliwiać integrację z Vmware vRealize Orchestrator. Wymienione aplikacje muszą rozpoznawać natywnie oferowaną macierz oraz intepretować jej statystyki.  Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: AIX, HP-UX, MS Windows, Vmware, Linux, Solaris.  Macierz musi mieć wsparcie dla automatycznego (T10 SCSI Unmap), bezagentowo, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012 i Windows 2016, VMFSv5 i v6 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning. |  |
|  | **Integracja z VMware** | Wraz z macierzą musi zostać dostarczone oprogramowanie do analityki end-to-end środowiska Vmware vSphere Zamawiającego korzystającego z zasobów oferowanej macierzy. Oprogramowanie musi:   * być dostępne dla administratora poprzez przeglądarkę WWW * Umożliwiać jednoczesną analizę co najmniej: pojedynczej maszyny wirtualnej, pojedynczego pliku VMDK, pojedynczego hosta ESXi, pojedynczego wolumenu macierzy   raportować następujące metryki w formie numerycznej i graficznej   * IOPS (operacje na sekundę) * Przepustowość na sekundę (MB/GB per second) * Opóźnienie (latencję) w ms * Obciążenie CPU i pamięci dla maszyn wirtualnych * Wskazywać w jednym oknie GUI korelację analizowanego komponentu z pozostałymi monitorowanymi komponentami środowiska Vmware. Komponentem jest VM, plik VMDK, host ESXi, Wolumen macierzy, Kontroler macierzy. * Raportować powyższe metryki historycznie na co najmniej 7 dni wstecz   Jeżeli do działania w/w oprogramowania wymagana jest licencja musi ona zostać dostarczona wraz z oprogramowaniem na pełną oferowaną pojemność macierzy ze wsparciem producenta na okres zgodny z gwarancją macierzy. |  |
|  | **Usługa utrzymania (serwisowa, gwarancyjna oraz wsparcia technicznego)** | Wykonawca zapewni dla wdrożonego systemu pamięci masowych, w okresie 36 miesięcy od dnia podpisania Protokołu Odbioru Technicznego, wsparcie techniczne na zasadach określonych poniżej.  Sprzęt i Oprogramowanie musi być objęte wsparciem serwisowym świadczonym w lokalizacji Zamawiającego w dni robocze (poniedziałek - piątek) w reżimie ‘Next Business Day’.  Sprzęt i Oprogramowanie musi być objęte wsparciem serwisowym świadczonym w lokalizacji Zamawiającego we wszystkie dni w reżimie ‘4-godz on-site’.  Zamawiający wymaga przedstawienia oświadczenie producenta że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Wsparcie techniczne dla Sprzętu i Oprogramowania będzie obejmować:   * Udostępnienie Zamawiającemu nowych wersji Oprogramowania w tym wszelkich poprawek, rozszerzeń oraz aktualizacji z chwilą publikacji. * Dostęp do internetowych stron pomocy technicznej producentów Oprogramowania. * Udzielanie odpowiedzi od Zamawiającego na pytania dotyczące aspektów operacyjnych/technicznych Sprzętu i Oprogramowania. * Zapewnienie stałego dostępu do zasobów elektronicznych (tj. dokumentacji) na temat Oprogramowania.   Zamawiający wymaga, aby w ramach świadczonej przez producenta gwarancji możliwe było przedłużanie okresu gwarancji minimalnie o miesiąc, przy czym miesięczna cena musi być stała niezmienna dla całego okresu gwarancji.  Zamawiający nie zwraca uszkodzonych dysków. |  |

**7) 3x serwer**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Spełnia** |
|  |  |  | **TAK/NIE** |
| Nazwa i model proponowanego rozwiązania:  …………………………………………………………………………………………………………………………………………………………………………………. | | | |
| **1.** | **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 2,5” * Obudowa wyposażona w panel LCD * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **2.** | **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Płyta główna posiadająca 32 sloty na kości pamięci * Płyta główna powinna obsługiwać do 8TB pamięci RAM. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Możliwość obsługi procesorów 40 rdzeniowych |  |
| **3.** | **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| **4.** | **Procesor** | * Zainstalowane dwa procesory min. 16-rdzeniowe, min. 3 GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 280 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **5.** | **RAM** | * Minimum 384GB DDR4 RDIMM 3200MT/s |  |
| **6.** | **Funkcjonalność pamięci RAM** | * Advanced ECC, * Memory Page Retire, * Fault Resilient Memory, * Memory Self-Healing lub PPR, * Partial Cache Line Sparing |  |
| **7.** | **Dyski twarde** | * Zainstalowane dwa dyski M.2 o pojemności min. 480GB z możliwością konfiguracji RAID 1. * Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |  |
| **8.** | **Zasilacze** | * Redundantne, Hot-Plug min. 1100W każdy. |  |
| **9.** | **Gniazda PCI** | * Min. 6 sloty PCIe generacji 4 |  |
| **10.** | **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Dodatkowa, dwuportowa karta sieciowa 25GbE SFP28 * Dodatkowa, dwuportowa karta FC 32Gb |  |
| **11.** | **Wkładki/kable** | * Nie wymagane |  |
| **12.** | **Porty** | * 4x USB w tym przynajmniej 1x USB 3.0 * 2x VGA w tym jedno z przodu serwera |  |
| **13.** | **System operacyjny/System wirtualizacji** | * Windows Server 2022 Datacenter, 16CORE per CPU |  |
| **14.** | **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |  |
| **15.** | **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **16.** | **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 V3 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| **17.** | **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |  |
| **18.** | **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   * + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **19.** | **Wspierane systemy operacyjne** | * Canonical® Ubuntu® Server LTS * Citrix® Hypervisor® * Microsoft® Windows Server® with Hyper-V * Red Hat® Enterprise Linux * SUSE® Linux Enterprise server * VMware® ESXi® |  |
| **20.** | **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. |  |
| **21.** | **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **22.** | **Warunki gwarancji** | * Gwarancji producenta: 3 lata * Możliwość rozszerzenia gwarancji przez producenta do 7 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w ciągu 4 godzin od otrzymania zgłoszenia. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Dla najwyższego poziomu ważności (1) zgłoszenia (awarii krytycznej) - zamawiający oczekuje natychmiastowego wysłania technika serwisowego, niezależnie czy diagnostyka została już zakończona. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. * Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. * Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   Możliwość rozszerzenia gwarancji o:   * Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:   + Monitorowanie zdarzeń w obrębie infrastruktury   + Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji * Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) * Zdalne lub na miejscu wdrażanie poprawek - 2x w roku * Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie) |  |

# 

# **8) 6x System operacyjny**

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Parametr | **Charakterystyka (wymagania minimalne)** | **Spełnia** |
| **TAK/NIE** |
| **1.** | **System operacyjny** | Przedmiotem zamówienia jest dostawa 6 sztuk licencji systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core. Licencje nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. |  |
| **2.** | **Licencje CAL** | 30 sztuk licencji dostępowych Microsoft Windows Server 2022 User CALs - 1 User CAL lub oprogramowanie równoważne. Licencje nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. |  |

**Opis równoważności dla Systemu Operacyjnego:**

**1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.**

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter, Zamawiający wymaga dostarczenia licencji dla 3 serwerów, oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię [ASP.NET](http://ASP.NET)
21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
22. Możliwość wykorzystania standardu http/2.
23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
26. Mechanizmy logowania w oparciu o: a) login i hasło,
    1. karty z certyfikatami (smartcard),
    2. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    1. określonych grup użytkowników,
    2. zastosowanej klasyfikacji danych,
    3. centralnych polityk dostępu w sieci,
    4. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji  
    w dokumentach (Digital Rights Management).
32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
       * + podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
         + ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
         + odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
         + bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
    3. zdalna dystrybucja oprogramowania na stacje robocze,
    4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
    5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
       * + Dystrybucję certyfikatów poprzez http,
         + Konsolidację CA dla wielu lasów domeny,
         + Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
         + Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    6. szyfrowanie plików i folderów,
    7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
    8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
    9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
    10. serwis udostępniania stron WWW,
    11. wsparcie dla protokołu IP w wersji 6 (IPv6),
    12. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    13. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
    14. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
    15. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover  
        z jednoczesnym zachowaniem pozostałej funkcjonalności.
    16. mechanizmy wirtualizacji mające wsparcie dla:
        * + dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
          + obsługi ramek typu jumbo frames dla maszyn wirtualnych.
          + obsługi 4-KB sektorów dysków,
          + nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
          + możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
    17. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
    18. wsparcie dla rozwiązania Kubernetes.
    19. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz  
        z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
    20. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
    21. mechanizmy deduplikacji i kompresji na wolumenach.
    22. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
    23. mechanizm konfiguracji połączenia VPN do platformy Azure.
    24. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
    25. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
    26. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

**Opis równoważności dla WINDOWS SERVER 2022 - USER CAL:**

**Zamawiający dopuszcza zaoferowanie produktów równoważnych do wyspecyfikowanej licencji Microsoft WINDOWS SERVER 2022 - USER CAL.**

**Minimalne wymagania dla licencji równoważnej:**

1. licencje równoważne muszą być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Microsoft Windows Server funkcjonującym u Zamawiającego,
2. licencje równoważne nie mogą zakłócić pracy środowiska systemowo - programowego Zamawiającego
3. licencje równoważne muszą w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie Microsoft Windows Server
4. licencje równoważne muszą zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem WINDOWS SERVER 2022 - USER CAL.
5. W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 5 godzin.

1. W przypadku zaoferowania przez Wykonawcę licencji równoważnych Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane licencje.

1. W przypadku, gdy zaoferowane przez Wykonawcę licencje równoważne nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu licencji równoważnych oraz dostarczy inne rozwiązana spełniające wymagania SOPZ.

1. Licencje równoważne dostarczane przez Wykonawcę nie mogą powodować utraty kompatybilności oraz wsparcia/gwarancji producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.

1. Licencje równoważne zastosowane przez Wykonawcę nie mogą w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie licencji równoważnych, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie licencji równoważnych, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

1. Zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

1. W przypadku dostarczania licencji, równoważnych względem wyspecyfikowanej przez Zamawiającego w Szczegółowym Opisie Przedmiotu Zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczone licencje spełniają wszystkie wymagania i warunki określone w Szczegółowym Opisie Przedmiotu Zamówienia.

# **Akcesoria sieciowe**

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Parametr | **Charakterystyka (wymagania minimalne)** | **Spełnia** |
| **TAK/NIE** |
| **1.** | **Patchcord RJ45** | 10 sztuk kabli 3 metrowych kat.6  10 sztuk kabli 2 metrowych kat.6 |  |
| **2.** | **Patchcord FTTH** | 6 sztuk światłowodów 3 metrowych MultiMod ze złączami LC-UPC/LC-UPC |  |
| **3.** | **Kable DAC** | 16 sztuk pasywnych kabli 3 metrowych DAC SFP28 |  |

1. **Wdrożenie**
   1. Macierz Dyskowa:
   * Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego
   * Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
   * Okablowanie sieciowe urządzeń
   * Uruchomienie i weryfikacja poprawności działania urządzeń
   * Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
   * Konfiguracja adresacji IP interfejsów zarządzania
   * Konfiguracja protokołu synchronizacji czasu NTP
   * Konfiguracja protokołu rozwiązywania nazw DNS
   * Instalacje niezbędnych licencji do uruchomienia wymaganych funkcjonalności
   * Integracja uwierzytelniania macierzy z domeną MS Active Directory
   * Konfigurację przestrzeni dyskowych zgodnie z wymaganiami Zamawiającego
   * Konfigurację interfejsów Front-End zgodnie z wymaganiami Zamawiającego
   * Konfiguracje mechanizmów zabezpieczeń przestrzeni dyskowych (snapshot)
   * Wykonanie testów działania nadmiarowości komponentów i poprawności konfiguracji w zakresie połączeń Front-End i odporności na zanik napięcia w jednym źródle zasilania
   1. Serwer RACK

* Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego
* Okablowanie sieciowe urządzeń
* Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
* Uruchomienie i weryfikacja poprawności działania urządzeń
* Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
* Konfiguracja adresacji IP interfejsów zarządzania
* Konfiguracja protokołu synchronizacji czasu NTP
* Konfiguracja protokołu rozwiązywania nazw DNS
* Weryfikacja poprawności działania połączeń LAN
* Wykonanie testów działania nadmiarowości zasilania i odporności na zanik napięcia w jednym źródle zasilania
  1. MS Active Directory
  + Instalacja systemu operacyjnego Windows Serwer 2022 Datacenter
  + Aktualizacja oprogramowania systemu operacyjnego do najwyższej rekomendowanej przez producenta wersji.
  + Uruchomienia usługi domeny MS Active Directory
  + Uruchomienie usługi serwera DNS
  + Uruchomienie usługi serwera DHCP
  + Dodanie do domeny 10 przykładowych stacji roboczych Zamawiającego.
  1. Dokumentacja powykonawcza
  + Przygotowanie dokumentacji powykonawczej z wdrażanych technologii i komponentów.

1. **Szkolenie**

Szkolenie pracowników Zamawiającego z zakresu zarządzania i utrzymania dostarczanego systemu wirtualizacji serwerów, macierzy dyskowej oraz zarządzania urządzeniami typu UTM:

* + minimum 24 godziny lekcyjne(45min),
  + Zamawiający po zakończonym szkoleniu wymaga przekazania materiałów dydaktycznych (prezentacja, skrypty ćwiczeń itp.) w języku polskim. Zamawiający dopuszcza przekazanie materiałów w formie nieedytowalnych plików PDF.