**Specyfikacja UTM szt. 2 w klastrze**

Producent: Model/Typ:

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, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Administrator ma mieć możliwość zdefiniowania niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy
i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu
o bazę LDAP (wewnętrzną lub zewnętrzną).
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System detekcji i prewencji włamań (IPS) ma wykrywać włamania oraz anomalie
w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
12. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
13. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
14. 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.
15. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
16. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
17. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
18. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
19. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
20. Urządzenie ma umożliwiać zastosowanie skanerów antywirusowego.
21. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
22. 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.
23. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
24. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
	1. IPSec VPN,
	2. SSL VPN.
25. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego
z oferowanym rozwiązaniem.
26. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
27. Urządzenie ma posiadać wbudowany filtr URL.
28. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowy.
29. W ramach filtra URL sklasyfikowanych jest co najmniej 100 milionów stron internetowych.
30. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie
w urządzeniu.
31. Administrator ma mieć możliwość dodawania własnych kategorii URL.
32. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

a) blokowanie dostępu do adresu URL,

b) zezwolenie na dostęp do adresu URL,

c) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

1. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron
z komunikatem o zablokowaniu strony.
2. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
3. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
4. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
5. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
6. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
	1. lokalną bazę użytkowników (wewnętrzny LDAP),
	2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
	3. usługę katalogową Microsoft Active Directory.
7. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory.
8. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
9. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
10. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu
o następujące dwa mechanizmy:
	1. równoważenie względem adresu źródłowego,
	2. równoważenie względem połączenia.
11. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
12. Urządzenie ma umożliwiać automatyczne przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego.
13. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
14. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
15. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
16. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej
o protokoły: RIPv2, OSPF oraz BGP.
17. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
18. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową,
a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
19. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
20. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów
z różnymi (także nakładającymi się) uprawnieniami.
21. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
22. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
23. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog)
z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
24. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
25. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
	1. manualnego eksportu do pliku w dowolnym momencie czasu,
26. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania
 i przeglądania logów zebranych na urządzeniu.
27. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
28. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
29. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1,2 i 3.
30. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
31. Urządzenie ma być objęte min.36 -miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji.
32. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
33. Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od potwierdzenia awarii.
34. Urządzenie mamusi pracować w trybie klastra wysokiej dostępności HA co najmniej
w trybie Active-Passive. Wymaga się dostarczenia 2 fizycznych tworzących klaster.
35. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB.
36. Liczba portów 2 x WAN min. 6 LAN
37. Urządzenie dedykowane wydajnościowo do obsługi klientów sieci LAN w ilości 100 stacji PC oraz 32 klientów VPN.
38. Przepustowość Firewall(1518 bajtów UDP)– minimum8Gbps.
39. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum3.3Gbps.
40. Przepustowość filtrowania Antywirusowego – minimum1 Gbps.
41. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum1.3Gbps.
42. Maksymalna liczba tuneli VPN IPSec – minimum500.
43. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu)– minimum 100.
44. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 75.
45. Obsługa interfejsów 802.11q(VLAN) – minimum256.
46. Urządzenie nie ma limitu na liczbę użytkowników.
47. Liczba reguł filtrowania – minimum 8 192.
48. Liczba tras statycznego routingu – minimum2 048.
49. Liczba tras dynamicznego routingu – minimum 10 000.
50. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.

Urządzenia należy dostarczyć zainstalować w miejscu eksploatacji mając na uwadze czynny obiekt i sieć szpitala. Wszelkie prace prowadzić tylko po wcześniejszym uzgodnieniu
i dokonaniu analizy i planu wdrożenia. Wymaga się szkolenia Administratora.

**Oprogramowanie do Wirtualizacji**

1. Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera
2. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
3. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 320 logicznych wątków oraz do 4TB pamięci fizycznej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych.
6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade).
Licencjonowanie nie może odbywać się w trybie OEM.
13. Rozwiązanie musi umożliwiać poprawne zainstalowanie następujących systemów operacyjnych: Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022 Windows 7, Windows 8, Windows 10, Windows 11, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 12.04, SCO OpenServer, SCO Unixware, Mac OS X
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance
16. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
17. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. Z możliwością wysyłania maila o wykonanej kopii bezpieczeństwa.
18. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
19. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
20. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych.
21. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
22. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności

HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

1. System musi posiadać funkcjonalność wirtualnego przełącznika (virtualswitch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.
2. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
3. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

Wymaga się zainstalowania oprogramowanie do Wirtualizacji, skonfigurowania oraz przeprowadzenia szkolenia dla Administratora

**System do kopii maszyn wirtualnych**

1. Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera
2. Zarządzanie poprzez GUI
3. System działający w modelu serwer – klient
4. Możliwość szyfrowania kopii po stronie klienta w celu zapewnienia bezpieczeństwa danych przed dotarciem do serwera backupowego
5. System backupowy posiada funkcjonalność deduplikacji
6. Możliwość korzystania z różnych typów przestrzeni dyskowych do składowania kopii bezpieczeństwa
7. System posiada funkcjonalność tworzenia harmonogramu wykonywania kopii
8. Automatyczna weryfikacja kopii bezpieczeństwa
9. Tworzenie kopii bezpieczeństwa maszyn wirtualnych
10. Możliwość tworzenia kopii na LTO-5 i nowsze
11. Powiadomienia e-mail o wykonanych / niewykonanych kopiach bezpieczeństwa
12. Możliwość zaplanowania maksymalnej liczy przechowywanych kopii

Wymaga się zainstalowania systemu do kopii maszyn wirtualnych, skonfigurowania oraz przeprowadzenia szkolenia dla Administratora.

**Oprogramowanie (licencja) na Windows Server 2022 PL Standard – zainstalowanego w roli kontrolera domeny Microsoft Active Directory na min. 50-100 użytkowników**

|  |
| --- |
| **Minimalne wymagane funkcjonalności** |
| Zamawiający wymaga, żeby serwerowy system operacyjny pochodził z oficjalnego kanału dystrybucji. |
| Zamawiający dopuszcza oferowanie oprogramowania i usług o szerszym zakresie funkcjonalnym od wymaganego |
| Serwerowy system operacyjny musi posiadać automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
| obsługa min. 8 core’ów fizycznych |
| Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe |
| zawarta możliwość uruchomienia roli serwera DHCP.zawarta możliwość uruchomienia roli serwera DNS.zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP). |
| możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. |
| Dostarczona licencja wieczysta musi pozwalać na przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu). |
| możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu. wsparcie techniczne będzie świadczone w języku polskim.W ramach wsparcia technicznego zapewniona będzie aktualizacja Oprogramowania, w tym niższe wersje (downgrade), wydania uzupełniające, poprawki programistyczne (patche).  |
| Możliwość pracy w roli klienta domeny Microsoft Active Directory. |
| zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. |
| Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. |
| Funkcja kompresji SMB umożliwiająca kompresowanie plików przesyłanych przez sieć. |
| zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022. |
| instalacja i użytkowanie aplikacji 32- oraz 64-bitowych na dostarczonym serwerowym systemie operacyjnym. |
| Licencja bez ograniczeń czasowych. Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na co najmniej jedną wersję niższą oraz z powrotem do wersji wyższej (przykładowo windows server 2022 na 2019 i z 2019 na 2022) z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer |
| wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami protokołów ip v4 i v6. |
| możliwość uruchomienia kontrolera domeny będącego w pełni zgodnym z domeną AD pracującą w oparciu o minimum system Windows Server 2022 (poziom funkcjonalności AD DS Windows Server 2022). |
| możliwość uruchomienia kontrolera domeny tylko do odczytu. możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny. |
| Wbudowane wsparcie instalacji i pracy na wolumenach, które umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
| możliwość uruchomienia serwera usług terminalowych (RemoteApp) zgodnego z min. Windows Server 2019/2022.  |
| obsługa zdalnego pulpitu.możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.obsługa PowerShell min. 6.0.obsługa certyfikatów w AD.możliwość podłączenia co najmniej 1 użytkowników zadalnie do serwera (poprzez RDP).Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.możliwość obsługi drzewa katalogowego Microsoft Active Directory. |
| Wsparcie techniczne (poprawki bezpieczeństwa, funkcjonalności itp.) producenta minimum 36 miesięcy od dnia podpisania Protokołu Odbioru Dostawy. |
| zawarta funkcjonalność szyfrowania dysków. |
| Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory. |
| Wykonawca zapewni dostęp do strony internetowej (portalu) pozwalającej upoważnionym osobom ze strony Zamawiającego co najmniej na obieranie zakupionego oprogramowania, aktywację zakupionego oprogramowania oraz sprawdzanie liczby zakupionych Produktów w wykazie zakupionych Produktów.Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.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), |
| Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu w rodzaju kosz systemowy.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. |
| wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją i zawarte w dostarczonej wersji programowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). |

Wymaga się zainstalowania kontrolera domeny Microsoft Active Directory, skonfigurowania oraz przeprowadzenia szkolenia dla Administratora.

|  |
| --- |
| Serwer szt. 2 w klastrze Producent: Model/Typ: |
| LP | Opis wymagania | Wymagane minimalne | **Parametry oferowanego produktu wpisać TAK/NIE lub opisać (Wykonawca powinien wskazać konkretne cechy w wykropkowanych miejscach)** | **Parametr oceniany** |
| 1 | Obudowa serwera | Obudowa Rack o wysokości max 2U z możliwością instalacji min.8 dysków 3.5" lub 2.5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Przedni paneli zamykanych na klucz, chroniących dyski twarde serwerów przed nieuprawnionym wyjęciem z serwerów. |  | brak oceny |
| 2 | Szafa rack | Serwery zostaną zainstalowane w dostarczonej szafie rack min 32U. |  | brak oceny |
| 3 | Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |   | brak oceny |
| 4 | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |   | brak oceny |
| 5 | Procesor | Dwa procesory dziesięciordzeniowe, klasy x86 dedykowane do pracy z zaoferowanym o taktowaniu bazowym nie niższym niż 3.1Ghz, w trybie turbo 4,1 GHz, TDP = 205W. Ze wsparciem dla technologii wirtualizacji lub równoważnych: VT-X, VT-d, VT-x with Extended PageTables (EPT) Osiągający w teście Passmark dostępnego na stronie https://www.cpubenchmark.net/minimum: 35356 punktów | Podać (marka/model) | brak oceny |
| 6 | RAM | 128 GB DDR4 RDIMM 2993MT/s, w modułach pamięci 32GB, na płycie głównej powinno znajdować się minimum 10 slotów przeznaczonych do instalacji pamięci. | Wpisać odpowiednio | Parametr oceniany 128 GB – 0 pkt 256GB – 10 pkt |
| 7 | Funkcjonalność pamięci RAM | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling – lub jednakowe występujące pod inną nazwą producenta. |   | brak oceny |
| 8 | Interfejsy sieciowe | 4 x RJ-45, GbE; 2 x SFP+, |   | brak oceny |
| 9 | Dyski twarde | Możliwość instalacji dysków SATA, SAS, SSD, serwer wyposażony w min. 4 dyski każdy o pojemności 1,92 TB SSD SAS HotPlug |  Wpisać odpowiednio | Parametr oceniany4 szt – 0 pkt; 6szt– 10 pkt |
| 10 | Kontroler RAID | Wbudowany, pamięć cache min 2gb konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 |   | brak oceny |
| 11 | Wbudowane porty  | min. 1 port USB 2.0, 1 port micro-USB oraz min. 3 porty USB 3.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), |   | brak oceny |
| 12 | Karta graficzna | Zintegrowana karta graficzna |   | brak oceny |
| 13 | Wentylatory | Redundantne, Hot-Plug |   | brak oceny |
| 14 | Zasilacze | Min. 2 redundantne, Hot-Plug min. 750W każdy, o sprawności min 94%  |   | brak oceny |
| 15 | Bezpieczeństwo | Zintegrowany moduł TPM 2.0, Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą |  | brak oceny |
| 16 | Diagnostyka | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze |   | brak oceny |
| 17 | Karta Zarządzania  | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: |   | brak oceny |
| zdalny dostęp do graficznego interfejsu Web karty zarządzającej |
| 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 SNMP; IPMI2.0, VLAN tagging, SSH |
| możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz |
| możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer |
| integracja z Active Directory |
| możliwość obsługi przez ośmiu administratorów jednocześnie |
| wsparcie dla automatycznej rejestracji DNS |
| wsparcie dla LLDP |
| wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej |
| możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy |
| monitorowanie zużycia dysków SSD |
| możliwość zdalnego ponownego uruchomienia lub włączania/wyłączania systemu oraz mapowania dysku wirtualnego do zdalnego udostępniania plików lub wdrażania systemu operacyjnego |
| możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON |
| automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram |
| możliwość przywrócenia poprzednich wersji firmware |
| automatyczne update firmware dla wszystkich komponentów serwera |
| 18 | Certyfikaty | Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog |   | brak oceny |
| 19 | Gwarancja  | Gwarancja producenta 3 lat, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać autoryzacje producenta urządzeń Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |  Wpisać odpowiednio | Parmetr oceniany 36 m-cy - 0pkt; 48 m-cy - 5 pkt; powyżej 48 m-cy - 10pkt |
| 20 | Dokumentacja  | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |   | brak oceny |
| 21 | Jakość wytworzenia | Serwer nie może być wyprodukowany później niż 12 miesięcy przed dostarczeniem. Nie dopuszcza się zaoferowania serwera lub jego komponentów odnawianego, demonstracyjnego lub powystawowego. Urządzenie musi być dostarczone z wszystkimi przewodami zasilającymi oraz logicznymi umożliwiającymi podłączenie serwera w serwerowni. |   | brak oceny |

Urządzenia należy dostarczyć zainstalować w miejscu eksploatacji mając na uwadze czynny obiekt i sieć szpitala. Wszelkie prace prowadzić tylko po wcześniejszym uzgodnieniu i dokonaniu analizy i planu wdrożenia. Wymaga się szkolenia Administratora.

|  |
| --- |
| Serwer plików do przechowywania backup'ów typu NAS Producent: Model/Typ: |
| LP | Opis wymagania | Wymagane minimalne | **Parametry oferowanego produktu wpisać TAK/NIE lub opisać (Wykonawca powinien wskazać konkretne cechy w wykropkowanych miejscach)** | **Parametr oceniany** |
| 1 | Rodzaj i liczba procesorów | min.1 nowoczesny czterordzeniowy i wydajny procesor o architekturze 64 bitowej zapewniajacy płynną obsługę danych składowanych przez zaproponowane rozwiązanie klastra serwerów HA |   | brak oceny |
| 2 | Obsługa pamięci masowych iSCSI | iSCSI Manager dający możliwości utworzenia i zarządzania: |   | brak oceny |
| • Maksymalna liczba iSCSI Target: 128 |
| • Maksymalna liczba jednostek iSCSI LUN: 256 |
| • Obsługa klonowania/migawek jednostek iSCSI LUN |
| 3 | Szyfrowanie | Mechanizn szyfrowania sprzętowego |   | brak oceny |
| 4 | Pamięć systemowa | min. 8 GB DDR4 |   | brak oceny |
| 5 | Całkowita min. liczba wolnych gniazd pamięci pod rozbudowę | 1 |   | brak oceny |
| 6 | Maksymalna obsługiwana pojemność pamięci | 32 GB |   | brak oceny |
| 7 | Kieszeń/kieszenie na dyski | min. 12 |   | brak oceny |
| 8 | Możliwość rozbudowy o moduły rozszerzające | min. 24 kieszenie na dyski |   | brak oceny |
| 9 | Moliwość zastosowania dysków | 3.5" SATA HDD 2.5" SATA HDD 2.5" SATA SSD |   | brak oceny |
| 10 | Dyski z możliwością wymiany podczas pracy (hot-swap) | TAK |   | brak oceny |
| 11 | Wymagana ilość dysków dostarczona z urządzeniem i ich rodzaj | Wymaga się dostawy zainstalowania wyłącznie dysków wymienionych na liście zgodności urządzenia . Wymaga się dostarczenia dysków min. **12 dysków** SATA o pojemności min. **2 T każdy**. |   | brak oceny |
| 12 | Port LAN RJ-45 1GbE | min. 2 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |   | brak oceny |
| 13 | Port USB 3.2 1. generacji | min. 2 |   | brak oceny |
| 14 | Obudowa (RU) | max 2U |   | brak oceny |
| 15 | Wspornik do montażu szafy | Zestaw Szyn do szafy typu rack 19”  |   | brak oceny |
| 16 | Tryb prędkości wentylatora | Tryb pełnej prędkości Tryb chłodzenia Tryb cichy |   | brak oceny |
| 17 | Przywracanie zasilania | TAK |   | brak oceny |
| 18 | Zaplanowane włączanie/wyłączanie | TAK |   | brak oceny |
| 19 | Funkcja Wake on LAN / WAN | TAK |   | brak oceny |

Urządzenia należy dostarczyć zainstalować w miejscu eksploatacji mając na uwadze czynny obiekt i sieć szpitala. Wszelkie prace prowadzić tylko po wcześniejszym uzgodnieniu
i dokonaniu analizy i planu wdrożenia. Wymaga się szkolenia Administratora.