Spis treści

[1. Serwer 2](#_Toc190851804)

[2. Router 6](#_Toc190851805)

[3. Macierz dyskowa 6](#_Toc190851806)

[4. Macierz dyskowa mała (serwer pod logi) 8](#_Toc190851807)

[5. System monitoringu IT 10](#_Toc190851808)

[6. Firewall sprzętowy 11](#_Toc190851809)

[7. UPS Sprzętowy 16](#_Toc190851810)

[8. Oprogramowanie wirtualizacyjne 17](#_Toc190851811)

[9. Oprogramowanie do zdalnego pulpitu 17](#_Toc190851812)

[10. Klucze sprzętowe 18](#_Toc190851813)

[11. Dysk zewnętrzny 18](#_Toc190851814)

[12. UPS dla urzędu i przedszkola 19](#_Toc190851815)

[13. Switch dla przedszkola 19](#_Toc190851816)

[14. Kontroler sieci dla przedszkola 20](#_Toc190851817)

[15. Szkolenia 21](#_Toc190851818)

[16. Wdrożenie 21](#_Toc190851819)

# Serwer

|  |  |  |  |
| --- | --- | --- | --- |
| ***Serwer*** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Obudowa** | Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 8 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. | | |
| **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | | |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | | |
| **Procesor** | Zainstalowane dwa procesory min. dwunasto-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 237 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. | | |
| **RAM** | Min. 128GB DDR4 RDIMM 4400MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. | | |
| **Gniazda PCIe** | - minimum trzy sloty PCIe x16  oraz jeden PCIe x8. | | |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10/25Gb Ethernet SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) | | |
| **Dyski twarde** | Możliwość instalacji dysków SAS/SATA  Zainstalowane: - 2 dyski min. 960GB SSD DWPD min. 1  - 2 dyski min. 480GB SSD DWPD min. 1  Zainstalowane dwa dyski M.2 NVMe o pojemności min. 480GB w konfiguracji RAID 1. | | |
| **Kontroler RAID/HBA** | Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60. | | |
| **Wbudowane porty** | Przednie: min. 1x VGA, min. 1x USB, min. 1x port dedykowany dla karty zarządzającej  Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, | | |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920 x 1200 | | |
| **Wentylatory** | Redundantne Hot-Plug | | |
| **Zasilacze** | Min. dwa zasilacze Hot-Plug maksymalnie 740W | | |
| **Serwerowy System Operacyjny** | Zamawiający wymaga dostarczenia oprogramowania Windows Server Standard Core 2022, licencja zgodna z oferowaną ilością rdzeni CPU w serwerze lub równoważne.  Opis równoważności poniżej. | | |
| **Bezpieczeństwo** | * 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 * TPM 2.0 * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. | | |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego która ma mieć możliwość na uruchomienie poniższych funkcjonalności:   * 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 podłączenia lokalnego poprzez złącze RS-232. * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. * Monitorowanie zużycia dysków SSD * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne update firmware dla wszystkich komponentów serwera * Możliwość przywrócenia poprzednich wersji firmware * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych * Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. | | |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.  Serwer musi posiadać deklarację zgodności UE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. | | |
| **Warunki gwarancji** | Pięć lat gwarancji producenta; czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia; możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do umowy oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.**  **Wymagane dołączenie do umowy oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.**  **Oświadczenie producenta serwera, jako załącznik do umowy, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.**  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. | | |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | | |
| **Serwerowy system operacyjny** | - Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.  - Licencja obejmująca wszystkie rdzenie procesorów w zaoferowanym serwerze.  - Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy:   1. Posiada możliwość wykorzystania min. 320 logicznych procesorów oraz min. 4 TB pamięci RAM w środowisku fizycznym 2. Posiada możliwość wykorzystywania min. 64 procesorów wirtualnych oraz min. 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Posiada możliwość budowania klastrów składających się z min. 64 węzłów,  z możliwością uruchamiania do 7000 maszyn wirtualnych. 4. Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:   - pozwalają na zmianę rozmiaru w czasie pracy systemu,  - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  - umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,  - umożliwiają zdefiniowanie list kontroli dostępu (ACL).   1. Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 2. Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 3. Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 4. Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 5. Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 6. Graficzny interfejs użytkownika. 7. Zlokalizowane w języku polskim, następujące elementy:   - menu,  - przeglądarka internetowa,  - pomoc,  - komunikaty systemowe.   1. Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 2. Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 3. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie  i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 4. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 5. Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   * + Podłączenie SSO 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.   - Zdalna dystrybucja oprogramowania na stacje robocze.  - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  - 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.  - Szyfrowanie plików i folderów.  - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami  i stacjami roboczymi (IPSec).  - Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.  - Serwis udostępniania stron WWW.  - Wsparcie dla protokołu IP w wersji 6 (Ipv6),  - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają 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,   - Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)  - Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.   1. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 2. Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 3. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 4. Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. | | |

# Router

|  |  |  |  |
| --- | --- | --- | --- |
| **Router** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Wysokość** | Max 1U | | |
| **Procesor** | Min.4 rdzenie o taktowaniu 1400 MHz | | |
| **Pamięć RAM** | Min. 1GB | | |
| **Pamięć flash** | Min. 512MB | | |
| **Porty** | Min. 10 x 10/100/1000 Ethernet oraz 1x SFP+ | | |
| **Zasilanie** | Maksymalny pobór urządzenia 33W | | |
| **Wsparcie dla IPsec** | Tak przyśpieszenie sprzętowe | | |
| **Wydajność IPsec** | Wydajność IPsec min. 67 Mbps przy szyfrowaniu AES-128-CBC + SHA1 oraz ramce 64 byte | | |
| **Normy** | CE, EAC, ROHS | | |
| **Gwarancja** | Min. 12 miesięcy | | |

# Macierz dyskowa

|  |  |  |  |
| --- | --- | --- | --- |
| **Macierz dyskowa** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U  i pozwalać na instalacje 24 dysków 2.5”. | | |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów iSCSi 10Gb Base-T. | | |
| **Cache** | Minimum 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. | | |
| **Dyski** | Zainstalowane 6 dysków Hot-Plug SAS SSD o pojemności 1.92TB oraz 18 dysków 2.4TB 10K RPM SAS.  Zaproponowane rozwiązanie musi wspierać instalację minimum 265 dysków w ramach jednego rozwiązania. | | |
| **Oprogramowanie/Funkcjonalności** | - Zarządzanie macierzą poprzez GUI oparte o HTML5.  - Wbudowany system powiadamiania drogą mailową o awarii.  - Macierz musi umożliwiać utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz. - Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 3TB.  - Wbudowana funkcjonalność automatycznego (bez interwencji człowieka) rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.  - Rozwiązanie musi posiadać funkcjonalność replikacji, minimum na poziomie replikacji asynchronicznej. Replikacja ta musi umożliwiać budowanie relacji w obu kierunkach.  Jeżeli którakolwiek z powyższych funkcjonalności wymaga dostarczenia dodatkowej licencji to należy ją zapewnić na całe oferowane rozwiązanie rozumiane w szczególności w zakresie przestrzeni dyskowej. | | |
| **Wsparcie dla systemów operacyjnych** | Windows Server 2019, Windows Server 2022, Red Hat Enterprise Linux (RHEL), SLES, Vmware. | | |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. Możliwość konfiguracji RAID 1, 5, 6, 10, ADAPT | | |
| **Warunki gwarancji** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, czas reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.  **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do umowy oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.**  **Wymagane dołączenie do umowy oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.**  **Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta stanowiące załącznik do umowy.**  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.  Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.  Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.  W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). | | |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim | | |
| **Certyfikaty** | Macierz musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.  Macierz musi posiadać deklarację zgodności UE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. | | |

# Macierz dyskowa mała (serwer pod logi)

|  |  |  |  |
| --- | --- | --- | --- |
| **Serwer na potrzeby logów** | | **Ilość** | **1 kpl.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Typ urządzenia** | Serwer NAS | | |
| **Obudowa** | Rack | | |
| **Procesor** | Czterordzeniowy procesor o taktowaniu 3,35 GHz (z przyspieszeniem do 3.6 GHz) | | |
| **Sprzętowy mechanizm szyfrowania** | Tak (AES-NI) | | |
| **Pamięć RAM** | min. 32 GB pamięci ECC UDIMM | | |
| **Przestrzeń dyskowa** | * Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap  z możliwością rozszerzenia do 24 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband | | |
| **Dyski twarde** | * **Urządzenie główne musi być wyposażone w min. 10szt. dysków twardych SATA 3.5”** klasy korporacyjnej o pojemności min. 8 TB każdy. Średni czas do awarii (MTBF) musi wynosić min. 2.5 mln godzin, prędkość przesyłu danych min. 260 MiB/s. * Dyski twarde muszą pochodzić od tego samego producenta co macierz główna celem zapewnienia pełnej kompatybilności na poziomie systemu operacyjnego oraz możliwości wykonywania aktualizacji oprogramowania układowego dysków z poziomu systemu NAS. | | |
| **Porty zewnętrzne** | Minimum:   * 2 porty USB 3.2 1. generacji * 1 gniazdo rozszerzenia | | |
| **Porty sieciowe** | Minimum:   * 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) * 1 port 10GbE RJ45 * 2 porty 10GbE SFP+ - Zamawiający dopuszcza zastosowanie dedykowanej karty sieciowej tego samego producenta co urządzenie główne | | |
| **Funkcja Wake on LAN/WAN** | Tak | | |
| **Gniazdo rozszerzeń PCIe 3.0** | Min. 1x 4-liniowe gniazdo x8 Gen. 3 | | |
| **Wentylator obudowy** | Min. 3 wentylatory 60 mm x 60 mm | | |
| **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV | | |
| **Obsługiwane systemy plików** | Min.:   * Wewnętrzny: Btrfs, ext4 * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT | | |
| **Zarządzanie pamięcią masową** | * Maksymalny rozmiar pojedynczego wolumenu:   + 200 TB (wymagana pamięć 32 GB)   + 108 TB * Minimalna liczba wewnętrznych wolumenów: 64 * Minimalna liczba obiektów iSCSI Target: 128 * Minimalna liczba jednostek iSCSI LUN: 256 * Obsługa klonowania/migawek jednostek iSCSI LUN | | |
| **Obsługiwane typy macierzy RAID** | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | | |
| **Funkcja udostępniania plików** | * Minimalna liczba kont użytkowników: 2 048 * Minimalna liczba grup użytkowników: 256 * Minimalna liczba folderów współdzielonych: 512 * Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 2 000 | | |
| **Uprawnienia** | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) | | |
| **Wirtualizacja** | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack® | | |
| **Usługa katalogowa** | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń. | | |
| **Bezpieczeństwo** | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) | | |
| **Obsługiwane przeglądarki** | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach | | |
| **Oprogramowanie** | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów  i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. * Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać  o 2 identyczne urządzenia. | | |
| **Konserwacja** | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych  w użyciu przesuwnych szyn rack | | |
| **Zasilanie** | * Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz | | |
| **Gwarancja** | Wykonawca udzieli gwarancji:   * 3 lata na urządzenie główne * 5 lat na dodatkowe kości RAM, kartę PCIe, dyski twarde * 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack | | |

# System monitoringu IT

|  |  |  |
| --- | --- | --- |
| **System monitoringu IT** | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | |
| 1. Architektura systemu    1. System musi mieć budowę modułową, składającą się z serwera zarządzającego, konsoli administracyjnej oraz agentów instalowanych na urządzeniach końcowych.    2. Oprogramowanie powinno umożliwiać komunikację między serwerem a agentami oraz konsolami administracyjnymi przy użyciu szyfrowanego protokołu (np. TLS 1.2 lub nowszego).    3. System powinien umożliwiać instalację wielu konsol zarządzania bez ograniczeń licencyjnych. 2. Monitorowanie infrastruktury IT    1. System musi umożliwiać bezagentowe monitorowanie urządzeń sieciowych (serwery Windows/Linux/Unix/Mac, routery, przełączniki, urządzenia VoIP, firewalle).    2. Oprogramowanie musi wspierać protokoły SNMP v1/2/3 oraz pułapki SNMP do monitorowania urządzeń sieciowych.    3. Wymagana obsługa wykrywania urządzeń w sieci oraz ich wizualizacji na mapach topologicznych.    4. System powinien umożliwiać monitorowanie serwisów TCP/IP, HTTP, FTP, SMTP, POP3, IMAP, SQL.    5. Wsparcie dla wirtualizacji (monitorowanie VMware). 3. Inwentaryzacja sprzętu i oprogramowania    1. Monitorowanie danych o konfiguracji sprzętowej (CPU, RAM, zajętość dysków, transfer sieciowy).    2. Monitorowanie zainstalowanego oprogramowania oraz audytowanie licencji.    3. Możliwość odczytu parametrów S.M.A.R.T. dysków SSD i HDD.    4. Obsługa ewidencji sprzętu IT z możliwością drukowania kodów alfanumerycznych.    5. Automatyczne wykrywanie i raportowanie zmian w konfiguracji sprzętu oraz oprogramowania. 4. Monitorowanie aktywności użytkowników    1. Rejestrowanie faktycznego czasu aktywności użytkowników.    2. Monitorowanie uruchamianych aplikacji i odwiedzanych stron internetowych.    3. Możliwość blokowania dostępu do aplikacji i stron WWW na poziomie użytkownika lub grupy.    4. Audyt wydruków (data, liczba stron, użytkownik, urządzenie).    5. Możliwość przechwytywania zrzutów ekranu użytkowników. 5. Zdalne zarządzanie i wsparcie użytkowników    1. Wbudowany moduł do obsługi zgłoszeń użytkowników.    2. Możliwość prowadzenia czatu wewnętrznego między użytkownikami i administratorami.    3. Funkcja zdalnego dostępu do komputerów użytkowników, z opcją przejęcia kontroli nad pulpitem. 6. Ochrona danych i kontrola nośników zewnętrznych    1. Możliwość blokowania urządzeń USB, Wi-Fi, Bluetooth, napędów optycznych, gniazd kart pamięci.    2. Monitorowanie operacji na plikach na dyskach lokalnych i zasobach sieciowych.    3. Audyt podłączanych nośników danych i prób użycia niezaufanych urządzeń.    4. Możliwość integracji z Windows Defender do monitorowania statusu zabezpieczeń. 7. Powiadomienia i alarmowanie    1. Możliwość definiowania reguł zdarzenie-akcja (np. restart serwera w przypadku wykrycia awarii).    2. Powiadomienia o zdarzeniach wysyłane na e-mail/SMS, z obsługą OAuth 2.0.    3. Możliwość integracji powiadomień z MS Teams i Slack. 8. Wymagania licencyjne    1. W ramach dostarczonego rozwiązania wymagane jest dostarczenie licencji umożliwiającej monitorowanie oraz zarządzanie infrastrukturą IT dla minimum 60 urządzeń.    2. Licencja musi obejmować pełną funkcjonalność systemu, bez dodatkowych opłat za poszczególne moduły.    3. Wsparcie techniczne oraz aktualizacje oprogramowania muszą być dostępne przez minimum 12 miesięcy.    4. Licencja nie może ograniczać liczby użytkowników administrujących systemem.    5. Licencja powinna umożliwiać łatwe rozszerzenie na większą liczbę urządzeń w przyszłości, bez konieczności przeinstalowania systemu. | | |

# Firewall sprzętowy

|  |  |  |  |
| --- | --- | --- | --- |
| **Firewall sprzętowy** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Wymagania Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. | | |
| **Redundancja, monitoring i wykrywanie awarii** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN. | | |
| **Porty komunikacyjne** | System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45, w tym:   * 2x RJ45 1GbE port WAN * 1x RJ45 1GbE port DMZ * 2x RJ45 1GbE port typu FortiLink * 5x RJ45 1GbE porty typu Internal Port   System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  System realizujący funkcję firewall musi być wyposażony w lokalną przestrzeń dyskową  o pojemności 128 GB.  W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. | | |
| **Parametry wydajnościowe** | W zakresie Firewall’a obsługa nie mniej niż: 1,4 miliona jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.  Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.  Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.  Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.  Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.  Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 800 Mbps.  Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps. | | |
| **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). | | |
| **Polityki, Firewall** | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP   W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hash'e złośliwych plików.  Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.   * Amazon Web Services (AWS) * Microsoft Azure * Google Cloud Platform (GCP) * OpenStack * VMware NSX | | |
| **Połączenia VPN** | System musi umożliwiać konfigurację połączeń typu IPSec VPN.  W zakresie tej funkcji musi zapewniać:   * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   System musi umożliwiać konfigurację połączeń typu SSL VPN.  W zakresie tej funkcji musi zapewniać:   * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. | | |
| **Routing i obsługa łączą WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. | | |
| **Funkcje SD-WAN** | System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu | | |
| **Zarządzanie pasmem** | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | | |
| **Ochrona przed malware** | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar.  System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.  System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. | | |
| **Ochrona przed atakami** | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.  Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.  System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.  Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | | |
| **Kontrola aplikacji** | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | | |
| **Kontrola WWW** | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.  Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.  W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | | |
| **Uwierzytelnianie użytkowników w ramach sesji** | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych  z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.   Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.  Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | | |
| **Zarządzanie** | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego  z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy  z dedykowanymi platformami centralnego zarządzania i monitorowania.  Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.  Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.  System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | | |
| **Logowanie** | Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania  i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych  o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.  Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych  i bezpieczeństwa oferowanego systemu.  Musi istnieć możliwość logowania do serwera SYSLOG. | | |
| **Dodatkowe elementy** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. | | |
| **Serwisy i licencje** | W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania  z aktualnych baz funkcji ochronnych producenta i serwisów.  Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. | | |
| **Gwarancja** | 24 miesiące gwarancji  Warunki szczegółowe:  Gwarancja musi być realizowana przez producenta sprzętu lub autoryzowany przez producenta serwis. Gwarancja producenta na dostarczone urządzenie polega na naprawie lub wymianie urządzenia w przypadku jego wadliwości.  W okresie obowiązywania gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania. | | |

# UPS Sprzętowy

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS Sprzętowy** | | **Ilość** | **11 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Moc znamionowa** | 800 VA / 480W | | |
| **Zakres napięcia wejściowego** | 170 ÷ 280V AC ± 7 % | | |
| **Czas podtrzymania** | 80% obciążenia minimum 2 minuty  50% obciążenia minimum 6 minut | | |
| **Czas przełączenia zasilania** | Max 6 ms | | |
| **Złącza wyjściowe** | minimum 2 gniazda z podtrzymaniem awaryjnym PN-E-93201 | | |
| **Zabezpieczenia** | Przeciwzwarciowe, przeciążeniowe | | |
| **Sygnalizacja** | Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe  i wyjściowe, poziom obciążenia, stan naładowania baterii | | |
| **Komunikacja** | Port USB | | |
| **Gwarancja** | min 24 miesiące na elektronikę i 12 miesięcy na akumulatory; | | |

# Oprogramowanie wirtualizacyjne

|  |  |  |
| --- | --- | --- |
| **Oprogramowanie wirtualizacyjne** | **Ilość** | **1 kpl.** |
| **Wymagane minimalne parametry techniczne** | | |
| Zamawiający wymaga dostarczenia oprogramowania wizualizacyjnego dla dostarczanego serwera. Dostarczane oprogramowanie wirtualizacje musi być objęte wsparciem technicznym dającym dostęp do repozytorium klasy Enterprise przez okres min. 5 lat.  Oferowane oprogramowanie musi wykorzystywać technologię wirtualizacji KVM i LXC.  Musi istnieć możliwość zarządzania z poziomu interfejsu web oraz CLI.  Interfejs zarządzania z poziomu przeglądarki musi być w języku polskim.  Oprogramowanie musi umożliwiać tworzenie klastrów wysokiej dostępności.  Oprogramowanie musi zapewniać obsługę sieciowych pamięci masowej:   * LVM Group (network backing with iSCSI targets) * iSCSI target * NFS Share * SMB/CIFS * Ceph RBD * Direct to iSCSI LUN * GlusterFS * CephFS   Oprogramowanie musi zapewniać obsługę lokalnych pamięci masowej:   * LVM Group * ZFS   Oferowane oprogramowanie musi posiadać interfejs webowy w języku polskim.  Oprogramowanie musi mieć wbudowane funkcjonalności: kopii zapasowej, zapory sieciowej, replikacji pamięci masowej.  Oprogramowanie musi umożliwiać tworzenie maszyn wirtualnych systemów Linux oraz Windows. | | |

# Oprogramowanie do zdalnego pulpitu

|  |  |  |
| --- | --- | --- |
| **Oprogramowanie do zdalnego pulpitu** | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | |
| 1. Parametry ogólne    1. Liczba użytkowników: 1    2. Jednoczesne połączenie: 1    3. Zarządzane urządzenia (dostęp nieautoryzowany): minimum 100    4. Liczba urządzeń, z których można nawiązać połączenie: minimum 3 2. Zdalny dostęp    1. Obsługa urządzeń mobilnych (Android i iOS)    2. Zdalny transfer plików    3. Zdalny restart    4. Zdalne drukowanie    5. Tunelowanie TCP: 1 port    6. Wake-On-LAN (zdalne wybudzanie urządzenia z trybu uśpienia) 3. Administracja    1. Alias niestandardowy pozwalający stworzyć przystępny w odbiorze identyfikator, który będzie używany zamiast domyślnego numeru ID.    2. Książka adresowa: minimum 1 książka adresowa z możliwością dodania minimum 100 wpisów    3. Nagrywanie sesji    4. Rejestrowanie sesji 4. Bezpieczeństwo    1. Uwierzytelnianie dwuskładnikowe (2FA)    2. Zapamiętywanie ustawień sesji    3. Niestandardowe profile uprawnień do sesji: minimum 3 profile    4. Tryb prywatności    5. Automatyczne rozłączanie 5. Współpraca    1. Czat tekstowy    2. Tablica    3. Zaproszenie do sesji 6. Wykonawca zobowiązany jest do dostarczenia licencji na okres dwóch lat, obejmującej pełen zakres funkcjonalności. | | |

# Klucze sprzętowe

|  |  |  |  |
| --- | --- | --- | --- |
| **Klucze sprzętowe** | | **Ilość** | **20 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Rodzaj urządzenia** | Klucz sprzętowy do uwierzytelniania | | |
| **Technologia** | Kryptografia asymetryczna (klucz publiczny) | | |
| **Protokoły** | U2F, FIDO2 | | |
| **Kompatybilność** | Obsługa uwierzytelniania dwuskładnikowego (2FA), logowania bezhasłowego oraz uwierzytelniania wieloskładnikowego | | |
| **Interfejs** | USB 2.0 | | |
| **Obsługa NFC** | Tak, możliwość uwierzytelniania za pomocą komunikacji bliskiego zasięgu | | |
| **Działanie offline** | Urządzenie nie może wymagać baterii ani dostępu do sieci | | |
| **Gwarancja** | 12 miesięcy | | |

# Dysk zewnętrzny

|  |  |  |  |
| --- | --- | --- | --- |
| **Dysk zewnętrzny** | | **Ilość** | **2 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Pojemność** | Min. 16TB | | |
| **Interfejs** | USB 3.2 Gen. 1 | | |
| **Złącza** | USB Typu-C  USB Typu-A | | |
| **Zabezpieczenia** | 256-bitowe szyfrowanie danych AES  Ochrona danych za pomocą klucza dostępu  Funkcja wykonywania kopii zapasowej | | |
| **Kompatybilność** | Kompatybilność z Windows i Mac OS | | |
| **Wymiary** | Maksymalne wymiary dysku: 200 mm x 131 mm x 47 mm | | |
| **Waga** | Maksymalnie 1,25 kg | | |
| **Gwarancja** | Minimum 24 miesiące | | |

# UPS dla urzędu i przedszkola

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS Sprzętowy** | | **Ilość** | **2 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Moc znamionowa** | 1200 VA / 600W | | |
| **Zakres napięcia wejściowego** | 170 ÷ 280V AC ± 7 % | | |
| **Czas podtrzymania** | 80% obciążenia minimum 4,5 minuty  50% obciążenia minimum 11 minut | | |
| **Czas przełączenia zasilania** | Max 6 ms | | |
| **Złącza wyjściowe** | minimum 2 x PN-E-93201 oraz 2 x IEC 320 C13 (10 A) | | |
| **Zabezpieczenia** | Przeciwzwarciowe, przeciążeniowe | | |
| **Sygnalizacja** | Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe i wyjściowe, poziom obciążenia, stan naładowania baterii | | |
| **Komunikacja** | Port USB | | |
| **Gwarancja** | min 24 miesiące na elektronikę i 12 miesięcy na akumulatory; | | |

# Switch dla przedszkola

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch dla przedszkola** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Wymiary** | Maksymalnie 450 mm x 45 mm x 205 mm | | |
| **Waga** | Maksymalnie 2.75 kg (bez uchwytów), 2.88 kg (z uchwytami rack) | | |
| **Przepustowość (non-blocking)** | Min. 25 Gbps | | |
| **Maksymalna przepustowość** | Min. 51 Gbps | | |
| **Maksymalny pobór mocy** | 25W | | |
| **Zasilanie** | 100-240VAC/50-60 Hz | | |
| **Zasilacz** | Wbudowany AC/DC | | |
| **Interfejsy** | 24x porty Gigabit Ethernet RJ45 10/100/1000 Mb/s  2x sloty SFP 1 Gb/s | | |
| **Interfejs zarządzania** | 1x RJ45 Serial Port Ethernet | | |
| **Certyfikaty** | CE, FCC, IC | | |
| **Montaż w szafie rackowej** | Tak, 1U | | |
| **Temperatura pracy** | Od -6 do 38° C | | |
| **Wilgotność pracy** | Od 12 do 90% (niekondensująca) | | |
| **Gwarancja** | Minimum 12 miesięcy | | |

# Kontroler sieci dla przedszkola

|  |  |  |  |
| --- | --- | --- | --- |
| **Kontroler sieci dla przedszkola** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| **Ilość portów LAN** | 8x 10/100/1000 Mb/s (RJ45)  1x 10 Gb/s (SFP+) | | |
| **Ilość portów WAN** | 1x 10/100/1000BaseTX (RJ45)  1x SFP+ (10 Gb/s) | | |
| **Typ obudowy** | Rack (1U) | | |
| **Zarządzanie** | Ethernet In-Band  Bluetooth BLE | | |
| **Wymiary** | Maksymalnie 445 mm x 44 mm x 287 mm | | |
| **Waga z uchwytami** | Maksymalnie 4,05 kg | | |
| **Przepustowość IDS / IPS** | Min. 3,5 Gb/s | | |
| **Procesor** | Min. 4-rdzeniowy procesor 1,7 GHz | | |
| **Pamięć systemowa** | Min. 4 GB DDR4 | | |
| **Wbudowana pamięć flash** | Min. 16 GB | | |
| **Zasilacz** | Wewnętrzny | | |
| **Gwarancja** | Minimum 12 miesięcy | | |

# Szkolenia

|  |  |  |  |
| --- | --- | --- | --- |
| **Szkolenia** | | **Ilość** | **1 szt.** |
| **Wymagane minimalne parametry techniczne** | | | |
| 1. **Szkolenie z serwera  i macierzy** | Wykonawca zobowiązany jest do zapewnienia szkolenia obejmującego pełną konfigurację  i zarządzanie wdrożonym serwerem oraz macierzą dyskową. Szkolenie ma obejmować zasady konfiguracji kontrolerów RAID, polityki zabezpieczeń, redundancję danych oraz optymalizację wydajności. Wykonawca musi zapewnić również omówienie metod monitorowania sprzętu, diagnostyki usterek oraz procedur konserwacyjnych i migracyjnych. | | |
| 1. **Szkolenie z konfiguracji  i zarządzania routerem** | Wykonawca zobowiązany jest do zapewnienia szkolenia przeprowadzonego przez profesjonalny podmiot zewnętrzny z dostarczanego rozwiązania, dotyczącego konfiguracji  i zarządzania routerem. Szkolenie musi obejmować podstawowe i zaawansowane funkcje zarządzania ruchem sieciowym, konfigurację polityk bezpieczeństwa, zarządzanie VPN oraz ochronę przed zagrożeniami. Wymagana jest również prezentacja narzędzi monitorujących oraz optymalizujących pracę routera. | | |
| 1. **Szkolenie z obsługi  i konfiguracji małej macierzy dyskowej (NAS)** | Wykonawca zobowiązany jest do zapewnienia szkolenia przeprowadzonego przez profesjonalny podmiot zewnętrzny z dostarczanego rozwiązania. Szkolenie musi obejmować wprowadzenie do linii produktowej urządzeń, początkową konfigurację systemu, zarządzanie przestrzenią dyskową oraz backup. Ponadto, należy omówić zagadnienia związane z usługami plików i folderów współdzielonych, snapshot replication, optymalizacją ustawień, funkcjami biznesowymi i bezpieczeństwa, konserwacją oraz migracją danych. | | |
| 1. **Szkolenie z obsługi  i konfiguracji systemu monitoringu IT** | Wykonawca zobowiązany jest do zapewnienia szkolenia przeprowadzonego przez profesjonalny podmiot zewnętrzny z dostarczanego rozwiązania obejmującego konfigurację  i zarządzanie systemem monitoringu IT. Szkolenie musi obejmować metody monitorowania infrastruktury IT, serwerów, aplikacji i stacji roboczych. Powinno również zawierać konfigurację powiadomień, automatyzację reakcji na incydenty oraz omówienie polityk raportowania  i analizy danych. | | |
| 1. **Szkolenie z firewall'a sprzętowego** | Wykonawca zobowiązany jest do zapewnienia szkolenia przeprowadzonego przez profesjonalny podmiot zewnętrzny z dostarczanego rozwiązania, dotyczącego konfiguracji  i zarządzania wdrożonym urządzeniem firewall. Szkolenie musi obejmować konfigurację polityk dostępu, filtrowanie ruchu sieciowego, integrację z VPN oraz ochronę przed zagrożeniami zewnętrznymi. Wymagana jest również nauka wykrywania i zapobiegania atakom sieciowym (IPS/IDS), a także procedury diagnostyczne i zabezpieczenia przed nieautoryzowanym dostępem. | | |

# Wdrożenie

1. Zakres wdrożenia

W ramach wdrożenia Wykonawca zobowiązany jest do kompleksowego uruchomienia i konfiguracji dostarczonego sprzętu oraz rekonfiguracji istniejącej infrastruktury IT Zamawiającego w sposób zapewniający pełną integrację i spójność systemową zgodnie z wytycznymi i we współpracy   
z Zamawiającym.

Wdrożenie musi zostać przeprowadzone poza godzinami pracy urzędu, tj. w godzinach nocnych,   
w weekendy lub w innych terminach uzgodnionych z Zamawiającym, tak aby nie zakłócać bieżącej działalności urzędu. Prace wdrożeniowe nie mogą ingerować w normalne funkcjonowanie urzędu   
w godzinach jego pracy. Oznacza to, że w trakcie standardowego czasu pracy wszystkie systemy i usługi muszą pozostawać dostępne dla pracowników i interesantów bez przerw i ograniczeń w działaniu.

W przypadku konieczności krótkotrwałego wyłączenia lub ograniczenia dostępu do jakichkolwiek usług, Wykonawca musi uzyskać uprzednią zgodę Zamawiającego oraz zapewnić alternatywne rozwiązania minimalizujące wpływ na pracę urzędu.

Zakres wdrożenia obejmuje m.in.:

* Montaż, konfigurację i integrację dostarczonych urządzeń (serwera, routera brzegowego, macierzy dyskowych, urządzeń sieciowych, firewalli, systemu monitoringu IT).
* Rekonfigurację istniejącego sprzętu IT tak, aby był w pełni zintegrowany z nową infrastrukturą.
* Instalację i konfigurację oprogramowania zarządzającego oraz systemów wspierających bezpieczeństwo i wydajność infrastruktury IT.
* Ułożenie i organizację wymaganych połączeń sieciowych i okablowania w sposób zgodny   
  z normami technicznymi.
* Przeprowadzenie testów kompatybilności z obecnym środowiskiem IT, zapewniających stabilność i wydajność wdrożonego rozwiązania.
* Sporządzenie dokumentacji powdrożeniowej, opisującej szczegóły konfiguracji, polityki bezpieczeństwa, plany awaryjne oraz procedury eksploatacyjne.

1. Wdrożenie klastra wysokiej wydajności

Wykonawca zobowiązany jest do wdrożenia klastra serwerowego, który będzie obsługiwał kluczowe usługi infrastruktury IT Zamawiającego. Zakres działań obejmuje:

* Określenie celów klastra, takich jak wysoka dostępność, równoważenie obciążenia oraz odporność na awarie.
* Konfigurację sieci i połączeń między serwerami, w tym ustawienie przełączników, routerów oraz zapewnienie odpowiedniej przepustowości i redundancji.
* Instalację i konfigurację systemu operacyjnego oraz oprogramowania zarządzającego klastrem.
* Ustawienie polityk failover, równoważenia obciążenia oraz skalowania, zapewniających nieprzerwaną pracę infrastruktury.
* Konfigurację pamięci masowej i systemów plików w sposób optymalizujący wydajność   
  i bezpieczeństwo danych.
* Implementację polityk bezpieczeństwa, w tym mechanizmów szyfrowania, systemów wykrywania i zapobiegania włamaniom (IPS/IDS) oraz firewalli.
* Przeprowadzenie testów wydajności oraz testów awaryjnych, symulujących różne scenariusze awarii oraz odzyskiwania systemu.
* Sporządzenie pełnej dokumentacji zawierającej architekturę systemu, schematy połączeń oraz procedury eksploatacyjne i awaryjne.

1. Wdrożenie serwera

W ramach wdrożenia serwera Wykonawca zobowiązany jest do:

* Montażu serwera w szafie rackowej i podłączenia do infrastruktury sieciowej.
* Konfiguracji interfejsów sieciowych i VLAN-ów, zapewniających optymalną łączność oraz segmentację ruchu.
* Instalacji systemu operacyjnego wraz z niezbędnymi aktualizacjami.
* Konfiguracji sprzętowych macierzy RAID, dostosowanych do wymagań wydajnościowych   
  i bezpieczeństwa.
* Konfiguracji polityk dostępu, użytkowników oraz systemów autoryzacji, zapewniających bezpieczne zarządzanie serwerem.
* Zabezpieczenia serwera przed zagrożeniami poprzez wdrożenie firewalli, systemów monitorowania oraz kontroli dostępu.
* Wdrożenia strategii backupu i odtwarzania danych z wykorzystaniem dedykowanych narzędzi.
* Przeprowadzenia testów obciążeniowych w celu weryfikacji wydajności i stabilności działania.
* Sporządzenia szczegółowej dokumentacji konfiguracji wraz z instrukcjami eksploatacyjnymi   
  i awaryjnymi.

1. Wdrożenie routera brzegowego

W ramach wdrożenia routera brzegowego Wykonawca zobowiązany jest do:

* Montażu urządzenia i jego podłączenia do sieci zgodnie z zaleceniami producenta.
* Konfiguracji interfejsów sieciowych, ustawień adresacji IP oraz routingu.
* Implementacji polityk bezpieczeństwa, w tym reguł firewall, NAT i VPN.
* Konfiguracji redundancji i przełączania awaryjnego (failover) w celu zapewnienia wysokiej dostępności.
* Wdrożenia mechanizmów QoS w celu optymalizacji ruchu sieciowego.
* Testowania konfiguracji pod kątem wydajności i zgodności z wymogami Zamawiającego.
* Sporządzenia dokumentacji technicznej i procedur awaryjnych.

1. Wdrożenie macierzy dyskowych

Wykonawca zobowiązany jest do pełnej konfiguracji dostarczonych macierzy, w tym:

* Montażu w szafie rackowej i podłączenia do infrastruktury.
* Konfiguracji systemu zarządzania pamięcią masową, w tym polityk RAID, LUN oraz dostępu do danych.
* Implementacji systemów ochrony danych, takich jak snapshoty, replikacja oraz szyfrowanie.
* Integracji z systemami backupu oraz strategii przywracania danych.
* Przeprowadzenia testów wydajności oraz walidacji systemów redundancji.
* Sporządzenia szczegółowej dokumentacji powdrożeniowej.

1. Wdrożenie systemu monitoringu IT

Wykonawca zobowiązany jest do:

* Instalacji i konfiguracji oprogramowania monitorującego zasoby sieciowe, serwery oraz stacje robocze.
* Konfiguracji alertów i powiadomień w celu automatycznej detekcji incydentów.
* Optymalizacji polityk monitorowania oraz automatyzacji reakcji na zdarzenia.
* Integracji systemu monitoringu z innymi elementami infrastruktury IT.
* Przeprowadzenia testów działania oraz zapewnienia poprawnej analizy logów i zdarzeń.

1. Instalacja i konfiguracja firewall'a sprzętowego

W ramach wdrożenia Wykonawca zobowiązany jest do:

* Instalacji urządzenia w infrastrukturze sieciowej oraz konfiguracji polityk zabezpieczeń.
* Implementacji mechanizmów filtrowania ruchu oraz systemów wykrywania zagrożeń (IPS/IDS).
* Integracji firewall'a z systemami monitorowania w celu zapewnienia spójnej strategii bezpieczeństwa.
* Testowania konfiguracji pod kątem skuteczności ochrony przed zagrożeniami oraz zgodności   
  z wymaganiami Zamawiającego.

1. Dokumentacja powdrożeniowa

Wykonawca zobowiązany jest do sporządzenia pełnej dokumentacji powdrożeniowej, obejmującej:

* Schematy połączeń sieciowych, topologię klastra oraz konfigurację sprzętu.
* Instrukcje administracyjne i procedury awaryjne.
* Polityki bezpieczeństwa oraz strategie zarządzania infrastrukturą.
* Dokumentację testów powdrożeniowych wraz z wynikami i rekomendacjami.

1. Testy końcowe

Po zakończeniu wdrożenia Wykonawca zobowiązany jest do przeprowadzenia kompleksowych testów systemu oraz monitorowania jego działania w celu potwierdzenia poprawności konfiguracji i zgodności z wymaganiami Zamawiającego.