Załącznik nr 1 do SWZ

**Szczegółowy opis przedmiotu zamówienia**

1. **Warunki realizacji zamówienia** 
   1. Wykonawca dostarczy urządzenia bezpośrednio do siedziby Urzędu Gminy:

**Urząd Gminy Łubniany, ul. Opolska 104, 46-024 Łubniany,**

* 1. Dostawa będzie uzgodniona szczegółowo pomiędzy Zamawiającym a Wykonawcą. Wykonawca zobowiązany jest we własnym zakresie zapewnić rozładunek elementów zamówienia,
  2. Wykonawca zapewni takie opakowanie sprzętu, jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego, jakości w trakcie transportu do miejsca dostawy.

1. **Specyfikacja ilościowa**:
   1. MONITOROWANIE INFRASTRUKTURY (licencja – 60 szt.);
   2. SERWER (1 szt.);
   3. WINDOWS SERVER STANDARD (1 szt.);
   4. WINDOWS SERVER CAL (15 szt.);
   5. SERWER NAS (3 szt.);
   6. UPS DO SERWERA RACK (1 szt.);
   7. NARZĘDZIA DO BACKUPU – KOPII ZAPASOWEJ (2 szt. – 1szt.: licencja na 14 komputerów, 1szt.: licencja na 7 komputerów);
   8. UTM (1 szt.);
   9. PRZEŁĄCZNIK PoE pod WIFI 24 porty (1 szt.) .
2. **Minimalne parametry techniczne i funkcjonalne:**
   1. **MONITOROWANIE INFRASTRUKTURY**

| **Parametr** | **Opis** |
| --- | --- |
| **Funkcja** | Musi zapewniać zbieranie szczegółowych informacji o sprzęcie, oprogramowaniu i użytkowaniu urządzenia oraz umożliwiać zdalne zarządzanie. |
| **Instalacja** | Powinna umożliwiać automatyczne wdrażanie na urządzenia końcowe w sposób niewidoczny dla użytkownika, z opcją dystrybucji poprzez Active Directory, skrypty instalacyjne lub ręczną instalację. |
| **Obsługiwane systemy operacyjne** | Musi być kompatybilny z systemami Windows od wersji XP do najnowszych edycji oraz zapewniać pełną funkcjonalność na wersjach serwerowych. |
| **Komunikacja z serwerem** | Powinna odbywać się przy użyciu szyfrowanych połączeń na dedykowanych portach TCP (np. 7288 dla synchronizacji z serwerem oraz 48084 dla komunikacji z konsolą zarządzającą). |
| **Obsługa zdalnego zarządzania** | Musi zapewniać możliwość przejęcia pulpitu zdalnego przez administratora IT, obsługiwać VNC na porcie TCP 48085 oraz umożliwiać zdalną instalację aplikacji, wykonywanie skryptów i kontrolowanie stanu urządzenia. |
| **Monitorowanie użytkowania systemu** | Powinno obejmować rejestrowanie uruchamianych aplikacji, odwiedzanych stron WWW, podłączanych urządzeń USB, sesji użytkownika oraz analizę ruchu sieciowego. |
| **Ochrona danych** | Musi zapewniać mechanizmy kontroli dostępu do urządzeń wymiennych, zabezpieczenie przed kopiowaniem danych na zewnętrzne nośniki oraz możliwość blokowania określonych działań użytkownika. |
| **Zabezpieczenia i polityki zgodności** | Powinny obejmować archiwizację logów, wykrywanie i alertowanie o nietypowych działaniach, integrację z politykami bezpieczeństwa oraz opcję audytowania aktywności użytkowników. |
| **Aktualizacje i konserwacja** | Musi umożliwiać automatyczne pobieranie i instalowanie aktualizacji poprzez serwer aplikacji oraz zapewniać opcję ręcznej synchronizacji dla natychmiastowego wdrożenia poprawek bezpieczeństwa. |
| **Integracja z systemami IT** | Powinna obejmować synchronizację z Active Directory, umożliwiać automatyczne przypisywanie użytkowników do określonych zasobów oraz wspierać import i eksport danych konfiguracyjnych. |
| **Zarządzanie zasobami** | Musi zapewniać szczegółowy wgląd w zasoby sprzętowe i oprogramowanie, obsługiwać raportowanie zmian konfiguracji oraz umożliwiać oznaczanie urządzeń na podstawie reguł organizacyjnych. |
| **Automatyzacja procesów IT** | Powinna obejmować możliwość tworzenia reguł dotyczących automatycznej reakcji na określone zdarzenia, planowania operacji administracyjnych i wymuszania polityk IT. |
| **Wydajność i optymalizacja** | Musi działać w sposób nieobciążający systemu operacyjnego, wykorzystywać minimalną ilość zasobów CPU i RAM oraz dynamicznie dostosowywać priorytet procesów w zależności od obciążenia urządzenia. |
| **Obsługa raportowania i logowania zdarzeń** | Powinna obejmować generowanie szczegółowych raportów dotyczących stanu urządzeń, użytkowania zasobów oraz statystyk bezpieczeństwa, a także umożliwiać ich eksport do formatów czytelnych dla narzędzi BI. |

* 1. **Serwer**

|  |  |
| --- | --- |
| **Parametr** | **Opis** |
| **Obudowa** | * Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3,5”. * Obudowa musi mieć możliwość 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. |
| **Płyta główna** | * Płyta główna z możliwością instalacji dwóch fizycznych procesorów, * Płyta główna posiadająca minimum 16 slotów na pamięć RAM RDIMM, * Płyta główna z możliwością zainstalowania do minimum 1TB pamięci RAM, * Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym. |
| **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowy klasy x86, min. 2.6GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 170 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **Pamięć RAM** | 128 GB pamięci RAM RDIMM o częstotliwości taktowania minimum 5600MHz |
| **Funkcjonalność pamięci RAM** | * Demand and patrol Scrubing * Failed DIMM isolation * Address parity protection |
| **Kontroler RAID** | * + Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. * Wsparcie dla dysków samoszyfrujących. |
| **Dyski twarde** | * Zainstalowane: * 2x dysk SSD SATA o pojemności min. 960GB, Hot-Plug * 2x dysk SAS 7.2k rpm o pojemności min. 4TB, Hot-Plug * Możliwość zainstalowania dwóch dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet BaseT |
| **Wbudowane porty** | * + Minimum 4 portów USB z czego min. 1 w technologii 3.0   + 1x VGA * Możliwość rozbudowy o port RS-232 |
| **Video** | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920x1200 pikseli |
| **Zasilanie** | Redundantne zasilacze o mocy minimum 700W klasy Titanium |
| **Diagnostyka i Bezpieczeństwo** | * Zintegrowany z płytą główną moduł TPM 2.0 V3 * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | * + Niezależna od zainstalowanego na serwerze systemu operacyjnego 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) |
| **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. * 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. * o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **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 potwierdzający spełnienie normy co najmniej Epeat Silver 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 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * + 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. |
| **Warunki gwarancji** | * + Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.   + Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.   + 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 rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.   + Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.   + Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.   + Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: * Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. * Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. * Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. * Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. * Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.   + Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * • 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. |

* 1. **Windows server**

| **Parametr** | **Opis** |
| --- | --- |
| **Typ licencji** | Jednorazowa płatność (perpetual license) |
| **Wersja systemu** | Windows Server 2025 Standard |
| **Model licencjonowania** | Licencja na rdzeń procesora (core-based licensing); minimum 16 rdzeni na serwer i 8 rdzeni na procesor |
| **Zarządzanie** | Active Directory, Group Policy, Server Manager |
| **Obsługiwane procesory** | Procesory 64-bitowe x64; minimum 1.4 GHz (2 GHz lub szybszy dla lepszej wydajności) |
| **Minimalna pamięć RAM** | 512 MB (RAM ECC dla lepszej stabilności) |
| **Minimalna przestrzeń dyskowa** | 32 GB dla instalacji systemu operacyjnego; dodatkowa przestrzeń wymagana dla serwerów DHCP, Active Directory itp. |
| **Maksymalna liczba rdzeni** | Brak ograniczeń dotyczących liczby rdzeni |
| **Maksymalna ilość pamięci RAM** | Obsługa do 24 TB pamięci RAM |
| **Wirtualizacja** | Hyper-V, obsługa do 2 maszyn wirtualnych + 1 host (licencja na instancje fizyczne i wirtualne) |
| **Usługi sieciowe** | DHCP, DNS, VPN, IP Address Management (IPAM), Network Controller |
| **Zarządzanie tożsamościami** | Active Directory Domain Services (AD DS), Active Directory Certificate Services (AD CS), Azure AD Integration |
| **Zarządzanie dostępem** | Just Enough Administration (JEA), Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA) |
| **Zarządzanie pamięcią** | Storage Spaces Direct, deduplikacja danych, ReFS (Resilient File System), obsługa technologii Storage Replica |
| **Zarządzanie bezpieczeństwem** | Windows Defender, Advanced Threat Protection (ATP), Secured-Core Server, BitLocker, SMB over QUIC, szyfrowanie SMB, Zasady Windows Defender Firewall |
| **Aktualizacje** | Windows Update for Business, wsparcie do 10 lat (5 lat wsparcia podstawowego i 5 lat wsparcia rozszerzonego) |
| **Współpraca z chmurą** | Integracja z Azure (Azure Arc, Azure Backup, Azure Site Recovery), Windows Admin Center |
| **Obsługa kontenerów** | Windows Containers, Linux Containers na Windows |
| **Wsparcie dla aplikacji** | .NET Core, ASP.NET, IIS, SQL Server, PowerShell 7 |
| **Rozszerzenia i role** | Usługi Active Directory (AD DS, AD CS, AD FS), Usługi plików i drukarek, Hyper-V, Usługi terminalowe, WDS (Windows Deployment Services) |
| **Kompatybilność sprzętowa** | Obsługa najnowszych urządzeń sprzętowych i technologii, takich jak PCIe Gen 4, NVMe, Direct Memory Access (DMA) |
| **Wsparcie techniczne** | Wsparcie Microsoft (wsparcie techniczne dostępne dla użytkowników z aktywną licencją) |

* 1. Windows server CAL

|  |  |
| --- | --- |
| **Parametr** | **Opis** |
| **Typ licencji** | Licencja na dostęp klienta (Client Access License - CAL), płatna jednorazowo |
| **Długość** **Rodzaje licencji CAL** | Licencje przypisane do użytkownika (User CAL) |
| **Model licencjonowania** | Jedna licencja CAL wymagana na każdego użytkownika lub urządzenie uzyskujące dostęp do serwera |
| **Zgodność z systemami** | Zgodne z Windows Server 2025, wsteczna kompatybilność z Windows Server 2019, Windows Server 2016 |
| **Funkcje licencji User CAL** | Przypisana do użytkownika; umożliwia jednemu użytkownikowi dostęp do serwera z dowolnego urządzenia (np. z laptopa, smartfona, komputera stacjonarnego) |
| **Zakres użytkowania** | Każdy użytkownik lub urządzenie łączące się z serwerem, korzystające z takich funkcji jak dostęp do plików, aplikacji, baz danych, usług drukowania, itp. |
| **Zastosowanie** | Dostęp do serwera dla użytkowników lub urządzeń w środowisku lokalnym (on-premise) |
| **Wymagania licencyjne dla maszyn wirtualnych** | CAL są wymagane dla każdego użytkownika/urządzenia uzyskującego dostęp do systemów operacyjnych na maszynach wirtualnych (VM) |
| **Wsparcie techniczne** | Licencje CAL uprawniają do korzystania ze wsparcia technicznego Microsoft, o ile są zgodne z warunkami licencyjnymi |
| **Dodatkowe usługi** | Dostęp do funkcji takich jak Active Directory, DNS, DHCP, File Services, Remote Access, IIS (Internet Information Services), Print Services |

* 1. **Serwer NAS**

|  |  |
| --- | --- |
| **Parametr** | **Opis** |
| **Typ obudowy** | Tower, 4-kieszeniowa macierz NAS |
| **Procesor** | Procesor czterordzeniowy o bazowej częstotliwości 2,0 GHz, osiągający do 2,7 GHz w trybie turbo. W teście PassMark CPU Mark uzyskał wynik 2 978 punktów. |
| **Liczba wątków** | 4 |
| **Pamięć podręczna CPU** | 4 MB Intel Smart Cache |
| **Obsługiwane instrukcje CPU** | Intel 64, VT-x, AES-NI, MMX, SSE, SSE2, SSE3, SSE4.1, SSE4.2 |
| **Pamięć RAM** | 2 GB DDR4 (rozszerzalne do 6 GB) |
| **Liczba slotów RAM** | 1 |
| **Maksymalna pojemność RAM** | 6 GB |
| **Liczba zatok na dyski** | 4x 3.5” HDD SATA + 2x M.2 2280 NVMe SSD |
| **Zainstalowane dyski HDD** | * 4x 4TB HDD SATA 3.5". * Interfejs SATA 6 Gb/s umożliwiający szybki transfer danych i kompatybilność z większością rejestratorów. * Technologia dostosowana do pracy 24/7 optymalizowana pod kątem ciągłego zapisu materiałów wideo. * Obsługa do 64 jednoczesnych strumieni wideo zwiększająca efektywność systemów monitoringu. * Zastosowanie technologii ograniczającej błędy rejestracji poprawiającej integralność danych. * Obroty 5400 RPM. * Pamięć podręczna o pojemności 64 MB wspomagająca płynność operacji zapisu i odczytu. * Zoptymalizowane zarządzanie energią zmniejszające zużycie prądu i emisję ciepła. * Ochrona przed wibracjami i wstrząsami dzięki specjalnym czujnikom minimalizującym wpływ warunków pracy. * Kompatybilność z rejestratorami NVR i DVR gwarantująca stabilność działania w różnych systemach monitoringu. * Wsparcie dla systemów sztucznej inteligencji umożliwiające analizę wideo w czasie rzeczywistym. * Odporność na wysokie temperatury pozwalająca na działanie w wymagających środowiskach pracy. * Technologia dynamicznego dostrajania buforu zapewniająca optymalne zarządzanie operacjami zapisu. * Średni czas bezawaryjnej pracy na poziomie miliona godzin świadczący o wysokiej trwałości. * Wsparcie dla standardowych formatów montażowych umożliwiające łatwą instalację w rejestratorach i serwerach NVR. * Kompatybilność z systemem operacyjnym zaoferowanego urządzenia oraz funkcjami magazynu danych .możliwa do potwierdzenia przez producenta urządzenia albo dostępna na stronach producenta |
| **Zainstalowane dyski SSD** | * 2x 1TB M.2 NVMe SSD. * Format M.2 2280 kompatybilny z dedykowanymi slotami w urządzeniu. * Interfejs NVMe PCIe 3.0 x4 gwarantujący wysoką przepustowość transferu danych. * Technologia pamięci 3D NAND zapewniająca większą trwałość i efektywność energetyczną. * Średnia prędkość odczytu do 3000 MB/s umożliwiająca szybkie operacje na dużych plikach. * Średnia prędkość zapisu do 1000 MB/s wspierająca dynamiczne przetwarzanie danych. * Współczynnik TBW=500 TB zapewniający długą żywotność nośnika. * Obsługa technologii cache SLC poprawiająca wydajność operacji zapisu. * Wsparcie dla funkcji TRIM i Garbage Collection zwiększających efektywność zarządzania pamięcią. * Zgodność z systemem plików Btrfs umożliwiająca optymalizację przechowywania i replikacji danych. * Zintegrowane funkcje korekcji błędów ECC gwarantujące bezpieczeństwo i integralność danych. * Obsługa szyfrowania AES-256 zapewniająca dodatkowy poziom ochrony informacji. * Kompatybilność z systemem operacyjnym zaoferowanego urządzenia oraz funkcjami magazynu danych .możliwa do potwierdzenia przez producenta urządzenia albo dostępna na stronach producenta * Zoptymalizowane pod kątem obsługi funkcji SSD Cache zwiększających wydajność pracy urządzenia * Niski pobór mocy wpływający na energooszczędność i ograniczenie generowanego ciepła * Odporność na wibracje i temperatury pracy od 0°C do 70°C zapewniająca stabilność działania w wymagających warunkach |
| **Maksymalna pojemność dyskowa** | 72 TB (z 4x 18TB HDD) |
| **Hot-swap** | Tak, dla zatok 3.5” |
| **Obsługiwane systemy plików** | Btrfs, EXT4 |
| **Obsługiwane poziomy RAID** | Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| **Snapshoty danych** | Tak, za pomocą Btrfs Snapshot Replication |
| **Interfejsy sieciowe** | 2x 1GbE RJ-45 |
| **Obsługa agregacji łączy** | Tak, Link Aggregation (IEEE 802.3ad) |
| **Obsługa VLAN** | Tak, IEEE 802.1Q |
| **Obsługa IPv6** | Tak |
| **Porty USB** | 2x USB 3.2 Gen 1 |
| **Obsługiwane protokoły sieciowe** | SMB, AFP, NFS, FTP, WebDAV, Rsync, SNMP |
| **System operacyjny** | * Oferowany system operacyjny powinien umożliwiać instalację aplikacji zgodnie z wykazem poniżej: * Moduł do zarządzania danymi umożliwiający tworzenie, edycję oraz udostępnianie plików w sieci lokalnej i poprzez Internet. * Aplikacja do synchronizacji plików pozwalająca na automatyczne kopiowanie i aktualizowanie zawartości między urządzeniami oraz chmurą. * Środowisko do tworzenia kopii zapasowych obsługujące różne metody zabezpieczenia danych, w tym replikację lokalną i zdalną. * System do zarządzania użytkownikami i dostępem umożliwiający tworzenie kont, grup, kontrolę uprawnień oraz integrację z zewnętrznymi systemami katalogowymi. * Platforma do obsługi wirtualizacji pozwalająca na uruchamianie i zarządzanie maszynami wirtualnymi oraz integrację z popularnymi środowiskami chmurowymi. * Oprogramowanie do przechowywania i analizy nagrań z kamer monitoringu, umożliwiające podgląd na żywo, nagrywanie i inteligentne wykrywanie zdarzeń. * System do obsługi kontenerów aplikacji, zapewniający możliwość uruchamiania lekkich środowisk programistycznych i testowych. * Moduł do obsługi multimediów, umożliwiający organizację, transkodowanie i strumieniowanie treści audio oraz wideo. * Serwer pocztowy pozwalający na konfigurację własnej skrzynki e-mail i zarządzanie korespondencją w firmowym środowisku. * System do automatycznego archiwizowania i organizacji zdjęć, oferujący funkcje rozpoznawania twarzy oraz kategoryzacji według treści. * Oprogramowanie do zarządzania bazami danych, umożliwiające uruchamianie i administrację systemami SQL oraz NoSQL. * Rozwiązanie do monitorowania zasobów i stanu systemu, zapewniające dostęp do logów, alertów oraz szczegółowych raportów wydajności. * Narzędzie do obsługi sieci VPN, pozwalające na konfigurację tuneli zabezpieczających połączenia zdalne. * System zarządzania tożsamością i uwierzytelnianiem, obsługujący logowanie wieloskładnikowe oraz integrację z zewnętrznymi usługami zabezpieczeń. * Aplikacja do automatyzacji zadań, umożliwiająca tworzenie harmonogramów oraz skryptów do zarządzania systemem i procesami biznesowymi. * Moduł integracji z platformami chmurowymi, umożliwiający synchronizację danych z zewnętrznymi usługami przechowywania i obliczeń. * Oprogramowanie do zarządzania treściami internetowymi, pozwalające na hostowanie stron oraz aplikacji webowych w bezpiecznym środowisku. * Rozwiązanie do zarządzania projektami i współpracy zespołowej, oferujące narzędzia do planowania, komunikacji i udostępniania dokumentów. * System analizy logów i zdarzeń, pozwalający na wykrywanie zagrożeń i generowanie raportów z aktywności użytkowników oraz systemu. * Platforma do obsługi automatycznego przesyłania i pobierania danych, wspierająca zaawansowane reguły filtrowania i harmonogramowanie operacji. * Zintegrowane środowisko do zarządzania siecią i konfiguracji zapór, pozwalające na monitorowanie ruchu i zabezpieczanie dostępu do systemu. * Oprogramowanie do szyfrowania i ochrony danych, wspierające mechanizmy zwiększające bezpieczeństwo przechowywanych informacji. * System zarządzania aktualizacjami, zapewniający automatyczną instalację poprawek i monitorowanie zgodności wersji systemu oraz aplikacji. |
| **Obsługa chmury** | Współdzielenie plików poprzez funckję Hybrid Share oraz Drive dostarczane przez producenta, Synchronizacja poprzez Cloud Sync z Google Drive, OneDrive i Dropbox. |
| **Zarządzanie użytkownikami** | Active Directory, LDAP, lokalne konta użytkowników |
| **Mechanizmy uwierzytelniania** | 2FA, certyfikaty SSL/TLS, VPN |
| **Ochrona danych** | Szyfrowanie AES-256, firewall, VPN Server, mechanizmy backupu |
| **Funkcje backupu** | Hyper Backup, Snapshot Replication, Active Backup for Businessy |

* 1. **UPS DO SERWERA RACK**

|  |  |
| --- | --- |
| **Parametr** | **Cecha/Wartość/Właściwość** |
| **Minimalne wymagania techniczne dla jednostki UPS** | * + Moc znamionowa jednostki nie mniej niż 1500VA / 1350W   + Konfiguracja faz 1:1   + Jednostka w obudowie Tower 2U z możliwością montażu w szafie Rack, szyny montażowe w zestawie   + Topologia line-interactive   + Temperatura eksploatacji 0 - 40 °C   + Wilgotność względna 20 - 90 %   + Wysokość n.p.m. podczas pracy 0-3000 m   + Słyszalny poziom hałasu: <40 dB w trybie normalnym, przy obciążeniu <70% / <45 dB w trybie AVR, przy obciążeniu >70%   + Sprawność ≥ 97% przy pełnym obciążeniu * Klasa ochrony IP 20 |
| **Parametry wejściowe** | * Nominalne napięcie wejściowe 230VAC   + Częstotliwość wejściowa 55–65 Hz (wykrywanie automatyczne)   + Typ gniazda wejściowego: * gniazdo IEC60320 C14   + Zmienny zakres napięcia wejściowego 166 - 278VAC * Ochrona przed przepięciami: 624J |
| **Parametry wyjściowe** | * + Napięcie wyjściowe 230VAC   + Inne napięcia wyjściowe 200, 208, 220, 230, 240   + Typ przebiegu sinusoida   + Złącza/gniazda wyjściowe * - 6x IEC 320 C13 (3 zarządzane) * Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny) |
| **Akumulatory i czas podtrzymania** | * Typ akumulatora: ołowiowo-kwasowy * Czas autonomii:   ≥ 6 minut dla pełnego obciążenia  ≥ 17 minut dla połowy obciążenia   * Typowy czas ładowania ≤3 godziny do 90% pojemności (od pełnego rozładowania) * Możliwość podłączenia do 6 zewnętrznych zestawów baterii * Baterie wymieniane na gorąco |
| **Komunikacja i zarządzanie** | * Gniazdo do montażu karty zarządzającej wspierającej SNMP oraz czujniki środowiska pracy * Wbudowane porty komunikacyjne: USB. * Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna pod postacią kolorowego ekranu LCD * Awaryjny wyłącznik zasilania (EPO) * Darmowe oprogramowanie do zamykania systemów operacyjnych |
| **Certyfikaty, zgodności oraz gwarancja** | * EN 62040-1:2008; * 3 lata gwarancji |

* 1. NARZĘDZIA DO BACKUPU – KOPII ZAPASOWEJ

|  |  |
| --- | --- |
| **Parametr** | **Opis** |
| **Obsługiwane systemy operacyjne** | Windows 7 i nowsze, macOS, Linux |
| **Typy kopii zapasowych** | Pełna, przyrostowa, różnicowa |
| **Metody backupu** | Backup plików i folderów, backup obrazów dysków |
| **Harmonogramy** | Możliwość planowania zadań backupu według ustalonych harmonogramów |
| **Szyfrowanie** | Szyfrowanie AES-256 zapewniające bezpieczeństwo danych |
| **Kompresja** | Opcje kompresji danych w celu oszczędności miejsca |
| **Zarządzanie** | Centralne zarządzanie poprzez konsolę webową |
| **Powiadomienia** | Konfigurowalne powiadomienia e-mail o statusie zadań backupu |
| **Wsparcie dla urządzeń mobilnych** | Aplikacje mobilne umożliwiające monitorowanie i zarządzanie |
| **Integracja z chmurą** | Obsługa różnych dostawców chmury do przechowywania kopii zapasowych |
| **Odzyskiwanie danych** | Opcje przywracania na poziomie plików oraz całych systemów |
| **Automatyczne aktualizacje** | Regularne aktualizacje zapewniające najnowsze funkcje i poprawki bezpieczeństwa |
| **Licencjonowanie** | Model subskrypcyjny z elastycznymi opcjami dostosowanymi do potrzeb użytkownika |

* 1. **UTM (Unified Threat Management)**

|  |  |
| --- | --- |
| **Parametr** | **Opis** |
| **Wymagania Ogólne** | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę 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 wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | * System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10x GE RJ45 ports (w tym 7x portów wewnętrznych, 2x porty WAN, 1x port DMZ). * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. * System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. * System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB. * System jest wyposażony w zasilanie AC; zasilanie 12V DC, 3A. |
| **Wydajność** | • Przepustowość IPS 1.4 Gb/s  • Przepustowość NGFW 1 Gb/s  • Przepustowość Threat Protection 700 Mb/s  • Przepustowość Firewalla (1518/ 512/ 64 bajty pakiety UDP) 10/ 10/ 6 Gb/s  • Opóźnienie zapory (64 bajtowe pakiety) 3.3 μs  • Przepustowość zapory (liczba pakietów na sekundę) 9 Mpps  • Sesje równoległe (TCP) 700 000  • Nowe sesje na sekundę (TCP) 35 000  • Firewall Policies 5 000  • Przepustowość IPsec VPN (512 bajtów) 6.5 Gb/s  • Tunele IPsec typu Brama-Brama 200  • Tunele IPsec typu Klient-Brama 500  • Przepustowość SSL-VPN 900 Mb/s  • Liczba użytkowników SSL-VPN (zalecana) 200  • SSL Inspection Throughput (IPS, avg. HTTPS) 630 Mb/s  • SSL Inspection CPS (IPS, avg. HTTPS) 400  • Ilość Sesji SSL Inspection (IPS, avg. HTTPS) 55 000  • Przepustowość kontroli aplikacji (HTTP 64K) 1.8 Gb/s  • Przepustowość CAPWAP (HTTP 64 KB) 8 Gb/s  • Domeny wirtualne (domyślne / maksymalne) 10/10  • Maksymalna liczba obsługiwanych przełączników FortiSwitches 16  • Maksymalna liczba FortiAP (łącznie/tunel) 64/32  • Maksymalna liczba FortiTokens 500  • Konfiguracje wysokiej dostępności Active/Active, Active/Passive, Clustering |
| **Funkcje Systemu Bezpieczeństwa** | * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). * Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. * Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| **Firewall oraz polityki bezpieczeństwa** | * Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. * System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. * Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. * Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. * •Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. * Element systemu realizujący funkcję Firewall integruje 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. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| **VPN** | 1.System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:   * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * •Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * 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. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   2.System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:   * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie zapewnia obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **Funkcje SD-WAN** | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Zarządzanie pasmem** | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  2. System daje możliwość określania pasma dla poszczególnych aplikacji.  3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.  4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **Ochrona przed malware** | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.  4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.  5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.  8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **Ochrona przed atakami** | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.  3. Baza sygnatur ataków jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  2. Baza Kontroli Aplikacji jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4.Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| **Kontrola WWW** | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.  4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.  9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1.System Firewall umożliwia 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.   2.System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  3.System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.  4.Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.  2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  4. Możliwość włączenia logowania per reguła w polityce firewall.  5. System zapewnia możliwość logowania do serwera SYSLOG.  6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **Weryfikacja parametrów** | Wszystkie funkcje i parametry wydajnościowe systemu muszą być możliwe do weryfikacji w oparciu publicznie dostępną dokumentację producenta albo wykonane testy. |
| **Gwarancja i aktualizacje** | System musi być objęty serwisem gwarancyjnym producenta realizowanym w trybie 24/7 przez 36 miesięcy licząc od daty uruchomienia urządzenia, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach serwisu producent zapewnia dostęp do aktualizacji oprogramowania przez 36 miesięcy licząc od daty uruchomienia urządzenia. |

* 1. **Przełącznik PoE**

|  |  |
| --- | --- |
| **Parametr** | **Cecha/Wartość/Właściwość** |
| **Parametry ogólne** | * Urządzenie musi być wyposażone w min. 24 gigabitowe porty RJ45 oraz min. cztery porty SFP+. Nie są dopuszczane porty SFP+ współdzielone z portami RJ45 (tzw. „combo”) * Porty SFP+ muszą również obsługiwać moduły pracujące z prędkością 1Gbps * Urządzenie musi posiadać port konsolowy RJ45 lub microUSB * Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward * Rozmiar tablicy adresów MAC urządzenia min. 16K * Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 128 Gbps * Min. szybkość przekierowań pakietów 95,2 Mpps * Urządzenie musi wspierać funkcjonalność PoE zgodną ze standardem 802.3af/at, minimalny wymagany budżet dostępny dla zasilanych urządzeń to 380W * Całkowity pobór mocy urządzenia (wliczając pełne obciążenie PoE) nie może przekraczać 490W * Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe   Głębokość urządzenia nie może przekraczać 450 mm |
| **Wspierane standardy** | 802.3i, 802.3u, 802.3z, 802.3ab, 802.3ad, 802.3ae, 802.3af, 802.3at, 802.3az, 802.3x, 802.1ab, 802.1d, 802.1w, 802.1s, 802.1p, 802.1q |
| **Funkcje** | * Zarządzanie za pomocą przeglądarki poprzez interfejs http/https * Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia * Obsługę stosu IPv4 i IPv6 * Funkcję wykrywania pętli * Funkcję izolacji portów * Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji) * Obsługę protokołu LLDP/LLDP-MED * Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 * Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) * Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) * Obsługę 4K identyfikatorów VLAN * Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) * IGMP Snooping oraz MLD Snooping * Obsługę min 500 grup multicastowych jednocześnie * MVR * Obsługę routingu statycznego i/lub dynamicznego * Możliwość konfiguracji co najmniej 16 interfejsów IP * Obsługę min 40 tras statycznych dla funkcji routingu statycznego * Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ * Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia * Obsługę list kontroli dostępu (ACL) * Obsługę SNMP w wersjach v1/v2c/v3   Obsługę grup RMON 1,2,3,9) |
| **Pozostałe wymagania** | * Urządzenie musi posiadać certyfikację CE * Gwarancja na urządzenie musi wynosić min. 5 lat   Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta |