

CZĘŚĆ II4 SWZ

DANE TECHNICZNE I WYPOSAŻENIE OFEROWANYCH
SERWERY

Nr postępowania: 2/KOM/2025

Wymagania Zamawiającego	Potwierdzenie spełnienia wymagań (tak/nie)	Parametry oferowanych stacji ładowania (UWAGA: należy wpisać faktyczne wartości parametrów oferowanych urządzeń i przyłączy oraz stacji ładowania)
<p><u>Serwer aplikacyjno-bazodanowy - 2 szt. spełniający poniższe wymagania:</u></p> <p>Obudowa Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz organizatorem kabli. Obudowa powinna umożliwiać instalację do 8 dysków 2,5".</p> <p>Procesor Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.4 GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 241 punktów base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.</p> <p>Liczba zainstalowanych procesorów 2</p> <p>Płyta główna Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje.</p> <p>Pamięć operacyjna Zainstalowane minimum 128 GB</p>		



<p>pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach 64 GB.</p> <p>Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.</p> <p>Zabezpieczenie pamięci Memory mirroring, ECC, SDDC.</p> <p>Procesor Graficzny Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.</p> <p>Dyski/Rozbudowa dysków W chwili dostawy serwer musi posiadać zainstalowane minimum 3 sztuki dysków HDD SAS 12 Gbps o pojemności minimum 600 GB, połączone za pomocą sprzętowego kontrolera RAID, nie zajmującego żadnego ze slotów PCIe (wspomnianych w pkt. „Sloty I/O PCIe”).</p> <p>Serwer powinien zawierać 8 wnęk na dyski, umożliwiające instalację nośników 2,5” hot-swap SSD/HDD w standardach SAS/SATA.</p> <p>Wymagany jest wewnętrzny slot na kartę Micro SD.</p> <p>Kontroler dyskowy W momencie dostawy serwer musi posiadać zainstalowany sprzętowy kontroler dyskowy, dedykowany przez producenta serwera.</p> <p>Kontroler powinien posiadać poziomy zabezpieczeń typu RAID 0, 1, 10, 5.</p> <p>Wymaga się obsługi globalnych dysków hot-spare.</p> <p>Karta HBA Zainstalowana karta z dwoma portami Mini-SAS HD x4 (SFF-8644).</p> <p>Zasilacz Minimum dwa zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.</p> <p>Interfejsy sieciowe Zainstalowana dwuportowa karta 10 Gb RJ-45. Karta nie może zajmować żadnego ze slotów PCIe.</p> <p>Sloty I/O PCIe Serwer powinien posiadać przynajmniej 2 sloty PCIe x16 generacji 5.</p> <p>Poza gniazdami PCIe dodatkowy slot OCP 3.0 PCIe 5.0 x16.</p> <p>Dodatkowe porty • z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem).</p>		
---	--	--

<p>Dedykowany port do diagnostyki dostępny z przodu serwera. Port VGA z przodu serwera.</p> <ul style="list-style-type: none"> • z tyłu obudowy: 2x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2. <p>Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płycie I/O, którą łączy się bezpośrednio z płytą główną serwera.</p> <p>Chłodzenie Wentylatory wspierające wymianę Hot-Swap, posiadające redundantne wirniki w każdym wentylatorze.</p> <p>Zarządzanie Wymaga się aby serwer posiadał port diagnostyczny z przodu obudowy umożliwiający podłączenie zewnętrznego panelu diagnostycznego LCD umożliwiającego detekcję usterek.</p> <p>Panel powinien umożliwiać wyświetlenie poniższych informacji:</p> <ul style="list-style-type: none"> • Aktywne ostrzeżenia • Status serwera • Typ oraz model serwera, numer seryjny • Wersje oprogramowania UEFI oraz modułu zarządzania • Informacje na temat modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS • Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii • Aktywne sesje połączeniowe do interfejsu zarządzania <p>Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty). Płyta I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Wymagane funkcjonalności kontrolera zdalnego zarządzania:</p> <ul style="list-style-type: none"> • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna) • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem 		
---	--	--

<p>systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.</p> <ul style="list-style-type: none"> • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie konsoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość zamontowania minimum 4 obrazów ISO jednocześnie w czasie jednej sesji • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • Możliwość zdefiniowania minimum 12 użytkowników lokalnych na karcie zarządzającej • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. 		
--	--	--

<p>Funkcje zabezpieczeń Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM 2.0. Możliwość instalacji przedniego panelu zabezpieczającego, zamykanego na klucz.</p> <p>Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji</p> <p>Urządzenia hot swap Dyski twarde, zasilacze, wentylatory.</p> <p>Obsługa Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser’ów PCIe, backplane’ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.</p> <p>Diagnostyka Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.</p> <p>Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.</p> <p>Systemy operacyjne Microsoft Windows Server 2019, 2022, 2025; Red Hat Enterprise Linux 9.5, SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3.</p> <p>Zainstalowany System Operacyjny Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz musi umożliwiać zainstalowanie 4 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.</p>		
---	--	--

<p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:</p> <ol style="list-style-type: none"> 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) 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) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> - 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). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 		
---	--	--



<p>12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET</p> <p>13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</p> <p>14) Wbudowana zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:</p> <ul style="list-style-type: none"> - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. <p>16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>18) Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> - Login i hasło, - Karty z certyfikatami (smartcard), - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), <p>19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..</p> <p>20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).</p> <p>21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów</p>		
---	--	--

<p>wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: <ul style="list-style-type: none"> o Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, o ii. Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, o iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. o iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. - 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: <ul style="list-style-type: none"> o Dystrybucję certyfikatów poprzez http o Konsolidację CA dla wielu lasów domeny, o Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen, o Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. - Szyfrowanie plików i folderów. - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). - Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. - Serwis udostępniania stron WWW. - Wsparcie dla protokołu IP w wersji 6 (IPv6), - Wsparcie dla algorytmów Suite B (RFC 4869), - 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 do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne 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 mają zapewnić wsparcie dla:

- o Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- o Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- o Obsługi 4-KB sektorów dysków
- o Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
- o Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- o Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

GWARANCJA: minimum 24 miesiące

Wraz z serwerami należy dostarczyć następujący komplet licencji dostępowych dla oferowanego systemu

operacyjnego:

a) 20 szt. licencji dostępowych na użytkownika

b) 20 szt. licencji dostępu zdalnego pulpitu na użytkownika

I. Macierz dyskowa - 1 szt. spełniająca

poniższe wymagania:

Obudowa Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19". Obudowa umożliwiająca instalację minimum 24 dyski 2,5" z możliwością wkładania i wyjmowania, bez wyłączania macierzy (dyski typu Hot Swap).

Pojemność: Macierz musi zostać dostarczona w konfiguracji zawierającej minimum: 12 dysków HDD 2,5" o pojemności minimum 1.8 TB każdy.

Macierz musi wspierać dyski:

- SSD: od 960GB do 15.36TB
- SAS: od 1.2TB do 2.4TB

Macierz musi mieć możliwość rozbudowy do minimum 96 dysków hot-swap.

Macierz musi być macierzą umożliwiającą jedoczesną konfigurację dysków SSD i SAS.

Kontroler Dwa kontrolery macierzy wyposażone w przynajmniej 8GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania baterijnego przez 72 godziny lub jako zrzut na pamięć flash. Zawartość cache musi być mirrorowana (kopia lustrzana) między kontrolerami.

Interfejsy Oferowana macierz musi posiadać minimum:

- 2 porty SAS 12 Gb/s, na kontroler,
- 1 port RJ-45 1 Gb Ethernet typu out-of-band management, na kontroler.
- 2 porty SAS 12 Gb/s do podłączenia dodatkowych półek, na kontroler.

Macierz musi pozwalać na wymianę w każdym kontrolerze 2 portów SAS na 4 porty SAS 12 Gb lub 4 porty 10/25 Gb iSCSI SFP28 lub 4 porty 16 Gb FC SFP lub 4 porty 32 Gb FC SFP bez potrzeby wymiany kontrolera macierzy.

RAID Kontrolery macierzy muszą umożliwiać konfigurację dysków w RAID: 0, 1, 5, 6, 10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 96 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.

Obsługiwane protokoły Macierz musi obsługiwać protokoły FC, iSCSI bez potrzeby wymiany kontrolerów

<p>macierzy (jedynie wymiana portów dla hostów).</p> <p>Inne Macierz musi posiadać wsparcie dla systemów: Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere.</p> <p>Macierz musi posiadać funkcjonalność wykonywania minimum 128 kopii migawkowych typu copy-on-write, z możliwością rozbudowy do 512 kopii migawkowych na system.</p> <p>Macierz musi posiadać możliwość replikacji danych po iSCSI lub FC w trybie asynchronicznym po zainstalowaniu dodatkowej licencji.</p> <p>Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.</p> <p>Macierz musi posiadać funkcjonalność thin provisioning.</p> <p>Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.</p> <p>Macierz musi zapewniać możliwość szyfrowania danych przy użyciu dysków typu FIPS SSD. Realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.</p> <p>Akcesoria 4 kable MiniSAS HD 8644/MiniSAS HD 8644 o długości min. 3 m.</p> <p><u>II. Serwer backupu/AD - 1 szt. spełniający poniższe wymagania:</u></p> <p>Obudowa Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz organizatorem kabli. Obudowa powinna umożliwiać instalację do 8 dysków 2,5".</p> <p>Procesor Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.4 GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 241 punktów base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.</p> <p>Liczba zainstalowanych procesorów 1</p>		
--	--	--

<p>Płyta główna Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje.</p> <p>Pamięć operacyjna Zainstalowane 128 GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach 64 GB. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.</p> <p>Zabezpieczenie pamięci Memory mirroring, ECC, SDDC.</p> <p>Procesor Graficzny Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.</p> <p>Dyski/Rozbudowa dysków W chwili dostawy serwer musi posiadać zainstalowane minimum 5 sztuk dysków HDD SAS 12 Gbps o pojemności minimum 1.2 TB, połączonych za pomocą sprzętowego kontrolera RAID, nie zajmującego żadnego ze slotów PCIe (wspomnianych w pkt. „Sloty I/O PCIe”). Serwer powinien zawierać 8 wnęk na dyski, umożliwiające instalację nośników 2,5” hot-swap SSD/HDD w standardach SAS/SATA. Wymagany jest wewnętrzny slot na kartę Micro SD.</p> <p>Kontroler dyskowy W momencie dostawy serwer musi posiadać zainstalowany sprzętowy kontroler dyskowy, dedykowany przez producenta serwera. Kontroler powinien posiadać poziomy zabezpieczeń typu RAID 0, 1, 10, 5. Wymaga się obsługi globalnych dysków hot-spare.</p> <p>Zasilacz Minimum dwa zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.</p> <p>Interfejsy sieciowe Zainstalowana dwuportowa karta 10 Gb RJ-45. Karta nie może zajmować żadnego ze slotów PCIe.</p> <p>Sloty I/O PCIe Serwer powinien posiadać przynajmniej 2 sloty PCIe x16 generacji 5.</p>		
---	--	--

Poza gniazdami PCIe dodatkowy slot OCP 3.0 PCIe 5.0 x16.

Dodatkowe porty • z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem). Dedykowany port do diagnostyki dostępny z przodu serwera. Port VGA z przodu serwera.

• z tyłu obudowy: 2x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9.

• wewnątrz obudowy: 1x USB 3.2.

Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płycie I/O, którą łączy się bezpośrednio z płytą główną serwera.

Chłodzenie Wentylatory wspierające wymianę Hot-Swap, posiadające redundantne wirniki w każdym wentylatorze.

Zarządzanie Wymaga się aby serwer posiadał port diagnostyczny z przodu obudowy umożliwiający podłączenie zewnętrznego panelu diagnostycznego LCD umożliwiającego detekcję usterek.

Panel powinien umożliwiać wyświetlenie poniższych informacji:

- Aktywne ostrzeżenia
- Status serwera
- Typ oraz model serwera, numer seryjny
- Wersje oprogramowania UEFI oraz modułu zarządzania
- Informacje na temat modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS
- Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii
- Aktywne sesje połączeniowe do interfejsu zarządzania

Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty). Płyta I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Wymagane funkcjonalności kontrolera zdalnego zarządzania:

- Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)
- Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja

<ul style="list-style-type: none"> • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie konsoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość zamontowania minimum 4 obrazów ISO jednocześnie w czasie jednej sesji • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • Możliwość zdefiniowania minimum 12 użytkowników lokalnych na karcie zarządzającej • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. 		
---	--	--

<ul style="list-style-type: none"> • Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. <p>Funkcje zabezpieczeń Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płycie I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM 2.0. Możliwość instalacji przedniego panelu zabezpieczającego, zamykanego na klucz.</p> <p>Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji</p> <p>Urządzenia hot swap Dyski twarde, zasilacze, wentylatory.</p> <p>Obsługa Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser’ów PCIe, backplane’ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.</p> <p>Diagnostyka Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.</p> <p>Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.</p> <p>Systemy operacyjne Microsoft Windows Server 2019, 2022, 2025; Red Hat Enterprise Linux 9.5, SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3.</p> <p>Zainstalowany System Operacyjny Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz musi umożliwiać zainstalowanie 2 instancji wirtualnych</p>		
---	--	--

<p>tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.</p> <p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:</p> <p>31) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</p> <p>32) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</p> <p>33) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.</p> <p>34) 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.</p> <p>35) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</p> <p>36) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</p> <p>37) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</p> <p>38) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</p> <p>39) Wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <ul style="list-style-type: none"> - 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). <p>40) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p>		
---	--	--

<p>41) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</p> <p>42) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET</p> <p>43) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</p> <p>44) Wbudowana zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>45) Dostępne dwa rodzaje graficznego interfejsu użytkownika:</p> <ul style="list-style-type: none"> - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, - Dotykowy umożliwiający sterowanie dotykkiem na monitorach dotykowych. <p>46) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>47) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>48) Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> - Login i hasło, - Karty z certyfikatami (smartcard), - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), <p>49) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..</p> <p>50) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).</p> <p>51) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>52) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>53) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>54) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych</p>		
--	--	--

środowiskach.

55) 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, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

- o Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

- o ii. Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

- o iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

- o iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

- 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:

- o Dystrybucję certyfikatów poprzez http

- o Konsolidację CA dla wielu lasów domeny,

- o Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,

- o Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

- Szyfrowanie plików i folderów.

- Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

- Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

- Serwis udostępniania stron WWW.

- Wsparcie dla protokołu IP w wersji 6 (IPv6),

- Wsparcie dla algorytmów Suite B (RFC 4869),

- Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na

<p>komputerach z systemem Windows,</p> <ul style="list-style-type: none"> - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne 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 mają zapewnić wsparcie dla: <ul style="list-style-type: none"> o Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, o Obsługi ramek typu jumbo frames dla maszyn wirtualnych. o Obsługi 4-KB sektorów dysków o Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra o Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. o Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) <p>56) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <p>57) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>58) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>59) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>60) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>61) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.</p> <p>GWARANCJA : minimum 24 miesiące</p> <p><u>Wraz z serwerem należy dostarczyć oprogramowanie do backupu spełniające poniższe wymagania:</u></p> <p>Wymagania ogólne</p> <p>Oprogramowanie musi być produktem przeznaczonym do</p>		
---	--	--

obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymagania : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Licencja wieczysta umożliwiająca wykonywanie kopii zapasowej minimum 5 maszyn wirtualnych.

Całkowite koszty posiadania

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.

Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

<p>Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla conajmniej trzech pamięci masowych to takiej puli.</p> <p>Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.</p> <p>Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.</p> <p>Oprogramowanie musi wspierać niezmiennosc kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.</p> <p>Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).</p> <p>Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji.</p>		
--	--	--

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.

Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora).

Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS).

Oprogramowanie musi posiadać integracje z systemami typu SIEM.

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

Wymagania RPO

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana

<p>funkcjonalność powinna działać w środowisku VMware.</p> <p>Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).</p> <p>Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).</p> <p>Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.</p> <p>Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.</p> <p>Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.</p> <p>Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.</p> <p>Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).</p>		
---	--	--

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

Wymagania RTO

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynie operatora, lub

<p>na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.</p> <p>Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.</p> <p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.</p> <p>Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.</p> <p>Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, enterprise applications oraz logi audytowe i sign-in.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych</p>		
---	--	--

<p>dokumentów wraz z historią ich wersji.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.</p> <p>Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.</p> <p>Ograniczenie ryzyka</p> <p>Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn</p>		
---	--	--

<p>wirtualnych.</p> <p>Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.</p> <p>Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.</p> <p>Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych.</p> <p>Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.</p> <p>Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.</p> <p>Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.</p> <p>Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise.</p> <p>Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR.</p>		
---	--	--

Środowiska fizyczne

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.

Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux.

Rozwiązanie musi wspierać system operacyjny macOS.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.

Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).

Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.

Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.

Rozwiązanie musi wspierać backup podłączonych dysków USB.

Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.

Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).

Rozwiązanie musi wspierać deduplikację oraz kompresję na

<p>źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone .</p> <p>Rozwiązanie musi wspierać kontrolę pasma sieciowego.</p> <p>Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.</p> <p>Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.</p> <p>Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.</p> <p>Rozwiązanie musi wspierać technologię BitLocker.</p> <p>Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.</p> <p>Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych.</p> <p>Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.</p> <p>Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.</p> <p>Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.</p> <p>Rozwiązanie musi wspierać szyfrowanie.</p> <p>Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium</p>		
---	--	--

<p>tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.</p> <p>Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.</p> <p>Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.</p> <p>Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.</p> <p>Monitoring</p> <p>System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.</p> <p>System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.</p> <p>System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.</p> <p>System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.</p> <p>System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.</p> <p>System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w</p>		
---	--	--

<p>celu centralnego monitorowania wielu środowisk.</p> <p>System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.</p> <p>System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.</p> <p>System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).</p> <p>System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.</p> <p>System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.</p> <p>System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.</p> <p>System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.</p> <p>System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.</p> <p>System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.</p> <p>Raportowanie</p> <p>System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi</p>		
---	--	--

<p>zarządzane przez konsole vCenter Server lub pracujące samodzielnie.</p> <p>System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.</p> <p>System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.</p> <p>System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.</p> <p>System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.</p> <p>System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.</p> <p>System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.</p> <p>System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.</p> <p>System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.</p> <p>System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.</p> <p>System musi mieć możliwość generowania raportów na</p>		
--	--	--

<p>podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.</p> <p>System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.</p> <p>System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.</p> <p>System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.</p> <p>System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).</p> <p>System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.</p> <p><u>III. Macierz NAS - 1 szt. spełniająca poniższe wymagania:</u></p> <p>Procesor 4-rdzeniowy/4-wątkowy.</p> <p>Obudowa Rack 2U wraz z szynami do montażu w szafie rack.</p> <p>Pamięć RAM 8 GB SODIMM DDR4. Możliwość rozbudowy do min. 16 GB.</p> <p>Ilość obsługiwanych dysków 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s.</p> <p>Gniazda M.2 Opcjonalnie przez kartę PCI-E.</p> <p>Interfejsy sieciowe 2 porty 2,5 Gigabit Ethernet (RJ45). 2 porty 10 GbE (10GBase-T).</p> <p>Porty USB 2 gniazda typu A USB 3.2 Gen 2 10 Gb/s.</p> <p>Porty PCIe 1 gniazdo PCI-E Gen 3.</p>		
---	--	--



<p>Wskaźniki LED HDD 1–8, stan, LAN.</p> <p>Obsługa RAID RAID 0, 1, 5, 6, 10, 50, 60.</p> <p>Protokoły SSH, Telnet, HTTP(S), FTP, CIFS/SMB, AFP.</p> <p>System plików Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+.</p> <p>Zasilanie Redundantne 300 W.</p> <p>Wentylatory 3 x 60mm.</p> <p>Zamontowane dyski 3.5" HDD 8 dysków o pojemności 8TB każdy SATA, zgodnych z listą kompatybilności proponowanego NAS.</p> <p><u>IV. Zasilacz awaryjny I - 1 szt. spełniający poniższe wymagania:</u></p> <p>Moc znamionowa zasilacza (VA/W) 6 000 VA / 6 000 W.</p> <p>Parametry zasilania wejściowego AC: Częstotliwość robocza, nominalna 50 lub 60 Hz (ustawienie fabryczne 50 Hz).</p> <p>Parametry zasilania wejściowego AC: Zakres napięcia 230 VAC.</p> <p>Parametry zasilania wejściowego AC: Okablowanie wejściowe Listwa zaciskowa.</p> <p>Parametry wyjścia AC: Gniazda wyjścia Listwa zaciskowa 2 (C19), 6 (C13).</p> <p>Parametry wyjścia AC: Fabrycznie VAC częstotliwość 230 VAC 50 Hz lub 60 Hz, nominalna.</p> <p>Parametry wyjścia AC: Kształt fali (podtrzymanie akumulatorowe) Sinusoida.</p>		
--	--	--

<p>Parametry wyjścia AC: Moc przeciążeniowa dla zasilania sieciowego (AC) > 150% przez minimum 200 ms; 125–150% przez 60 sekund; 105–125% przez 5 minut; ≤ 105 % ciągłe.</p> <p>Akumulator: Typ Szczelny, regulowany zaworowo, ołowiowo-kwasowy.</p> <p>Akumulator: Czas podtrzymania akumulatorowego (przy 100% obciążeniu) 5 minut.</p> <p>Akumulator: Czas podtrzymania akumulatorowego (przy 50% obciążeniu) 13 minut.</p> <p>Wyposażenie Zestaw do montażu w szafie rack. Karta sieciowa do zarządzania SNMP i poprzez sieć.</p> <p><u>V. Zasilacz awaryjny II - 1 szt. spełniający poniższe wymagania:</u></p> <p>Moc znamionowa zasilacza (VA/W) 10 000 VA / 10 000 W.</p> <p>Parametry zasilania wejściowego AC: Częstotliwość robocza, nominalna 50 lub 60 Hz (ustawienie fabryczne 50 Hz).</p> <p>Parametry zasilania wejściowego AC: Zakres napięcia 230 VAC.</p> <p>Parametry zasilania wejściowego AC: Okablowanie wejściowe Listwa zaciskowa (wspólna lub rozdzielone obejście).</p> <p>Parametry wyjścia AC: Gniazda wyjścia Listwa zaciskowa 4 (C19), 4 (C13).</p> <p>Parametry wyjścia AC: Fabrycznie VAC częstotliwość 230 VAC 50 Hz lub 60 Hz, nominalna.</p> <p>Parametry wyjścia AC: Kształt fali (podtrzymanie akumulatorowe) Sinusoida.</p>		
--	--	--

<p>Parametry wyjścia AC: Moc przeciążeniowa dla zasilania sieciowego (AC) > 150% przez minimum 200 ms; 125–150% przez 60 sekund; 105–125% przez 5 minut; ≤ 105 % ciągle.</p> <p>Akumulator: Typ Szczelny, regulowany zaworowo, ołowiowo-kwasowy.</p> <p>Akumulator: Czas podtrzymania akumulatorowego (przy 100% obciążeniu) 19 minut (dopuszczalne dodatkowe moduły bateryjne).</p> <p>Akumulator: Czas podtrzymania akumulatorowego (przy 50% obciążeniu) 48 minut (dopuszczalne dodatkowe moduły bateryjne).</p> <p>Wypożyczenie Zestaw do montażu w szafie rack. Karta sieciowa do zarządzania SNMP i poprzez sieć.</p> <p><u>VI. Przełącznik sieciowy - 4 szt. spełniający poniższe wymagania:</u></p> <p>Porty 10G/Multi-Gigabit RJ45 (10G/5G/2.5G/1G) 16 szt.</p> <p>Porty 10G SFP+ 2 szt.</p> <p>Przepustowość 360 Gbps.</p> <p>Maks. liczba tablicy MAC 16K.</p> <p>Rozmiar bufora 4 MB.</p> <p>Liczba obsługiwanych sieci VLAN 512.</p> <p>Routing VLAN Tak.</p> <p>Dynamiczne przypisywanie VLAN Tak.</p> <p>MLD Snooping Tak.</p> <p>Routing statyczny Tak.</p>		
--	--	--

Tabela ARP hosta 1024.

Zapobieganie atakom DoS Tak.

Zasilacz Wewnętrzny.

Wyposażenie Zestaw do montażu w szafie rack.

VII. Urządzenie ochrony sieci UTM - 1 szt. spełniające poniższe wymagania:

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 5 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

1. 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.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.

4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1.3 Gbps.
5. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. 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.
4. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
5. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
6. Rozwiązywanie 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).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. 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.

3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.

5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

7. 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.

Połączenia 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

<p>Mesh.</p> <ul style="list-style-type: none"> • 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. <p>2. 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.</p> <p>Routing i obsługa łączy WAN</p> <p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv3), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. <p>Funkcje SD-WAN</p> <ol style="list-style-type: none"> 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 		
--	--	--



<p>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p> <p>Zarządzanie pasmem</p> <p>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>2. System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p> <p>Ochrona przed malware</p> <p>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <p>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.</p> <p>8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>		
---	--	--

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. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
7. 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. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. 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.

<p>3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji</p> <p>Uwierzytelnianie użytkowników w ramach sesji</p> <p>1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • 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. <p>2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.</p> <p>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.</p> <p>4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p> <p>Zarządzanie</p> <p>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.</p> <p>2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z</p>		
--	--	--

<p>wykorzystaniem szyfrowanych protokołów.</p> <p>3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.</p> <p>4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p> <p>Logowanie</p> <p>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.</p> <p>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.</p> <p>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>4. Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>5. System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p> <p>Serwisy i licencje</p> <p>1. Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web</p>		
--	--	--

Filtering.			
<u>VIII. Szafa rack - 1 szt. spełniająca poniższe wymagania:</u>			
Wysokość	42U.		
Szerokość	600 mm.		
Głębokość	1000 mm.		
Drzwi przednie	Perforowane.		
Drzwi tylne	Perforowane.		
Ściany boczne	Pełne.		
Belki nośne	Dwie pary belek w rozstawie 19".		
<u>IX. Przełącznik KVM - 1 szt. spełniający poniższe wymagania:</u>			
Połączenia komputera Bezpośrednie: 8. Maksymalnie: 64 (połączenie kaskadowe).			
Wybór portu	Menu ekranowe, skróty klawiszowe, przyciski.		
Złącza Porty konsoli: 1 x SPHD-18 męskie. Porty KVM: 8 x SPHD-15 żeńskie. Aktualizacja oprogramowania układowego: 1 x gniazdo RJ-11. Zasilanie: 1 x gniazdo DC.			
Emulacja	Klawiatura/Mysz: PS/2, USB.		
Wideo	2048 x 1536; DDC2B.		
Odstęp czasu skanowania	1–255 sekund (domyślnie: 5 s).		
Wyposażenie Zestaw do montażu w szafie rack. 3 kable USB o długości min. 3 m każdy do połączenia konsoli z			



serwerami.		
------------	--	--

GWARANCJA: minimum 24 miesiące.		
--	--	--

