Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia jest dostawa fabrycznie nowych, nieużywanych urządzeń, pochodzących z oficjalnej i bieżącej dystrybucji producenta elementów infrastruktury IT, zgodnie z poniższym zestawieniem:
2. **Serwer przeznaczony do montażu w szafie rack 19’’ – 2 sztuki**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne)*** |
| 1. | Ilość procesorów | 1 szt. co najmniej 16-rdzeniowy, do zastosowań serwerowych | **Producent/model procesora:**  **……………………………** |
| 2. | Architektura procesora | 64-bit |  |
| 3. | Wydajność procesora | co najmniej 29 000 punktów w teście wydajnościowym PassMark CPU Benchmarks. Wyniki testu będą weryfikowane pod adresem: https://www.cpubenchmark.net/cpu\_list.php. |  |
| 4. | Obudowa: | Rack 19” o wysokości max 1U. |  |
| 5. | Pamięć | 128 GB DDR5 o taktowaniu nie mniejszym niż 4800 MT/s |  |
| 6. | Zamontowane dyski (system) | 2,5’’ 480 GB SSD M.2 NVMe – 2 szt. |  |
| 7. | Karty sieciowe: | * 1. 4-portowa RJ-45 GbE,   2. 2-portowa SFP28, 25 Gb/s,   3. 2-portowa LC, 32 Gb/s, Fibre Channel. |  |
| 8. | Porty komunikacyjne: | USB 3.0 – 1 szt, USB 2.0– 2 szt, VGA – 1 szt., port zarządzania |  |
| 9. | Wymagane cechy funkcjonalne serwera: | obudowa serwera musi zostać dostarczona wraz z ramką zabezpieczającą przed nieautoryzowanym dostępem do dysków znajdujących się na froncie urządzenia |  |
|  |  | serwer musi oferować minimum dwa sloty PCIe x8 generacji 4, |  |
|  |  | serwer musi umożliwiać zainstalowanie co najmniej: 4 szt. dysków 3.5" oraz do 8 szt. dysków 2.5" lub 16 szt. zatok dla dysków NVMe, |  |
|  |  | serwer musi umożliwiać instalację minimum dwóch portów 25GbE SFP28, |  |
|  |  | niezależnie od zainstalowanego na oferowanym serwerze systemu operacyjnego urządzenie musi posiadać dedykowany port zarządzający, nie pełniącym jednocześnie innej funkcji, typu RJ-45 Gigabit Ethernet umożliwiający:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej, * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, * podmontowanie zdalnych wirtualnych napędów, * wirtualną konsolę z dostępem do myszy, klawiatury, * wsparcie dla IPv6, SNMP, LLDP, IPMI2.0, VLAN tagging, SSH, * zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer, * integracje z Active Directory, * wspierać obsługę przez więcej niż jednego administratora jednocześnie, * wysłanie do administratora wiadomości mailowych zawierających powiadomienie o awarii lub zmianie konfiguracji sprzętowej, * monitorowanie zużycia dysków SSD, * automatyczny update firmware dla wszystkich komponentów serwera, * możliwość przywrócenia poprzednich wersji firmware, * możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOS, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON, * możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych, * automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. |  |
|  |  | serwer musi zostać wyposażony we wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą, |  |
|  |  | serwer musi umożliwiać wyłączenie portów USB znajdujących się na obudowie oraz wyłączenie przycisku zasilania |  |
|  |  | serwer musi być wyposażony w moduł TPM (Trusted Platform Module) w wersji 2.0 |  |
|  |  | serwer musi być wyposażony w sprzętowy kontroler dyskowy, umożliwiający konfigurację RAID 0, 1, 5, 6, 10, 50 oraz 60. Kontroler musi zapewniać obsługę dysków twardych i SSD typu SAS3 oraz SATA III, |  |
|  |  | serwer musi być wyposażony w dodatkowy moduł przeznaczony dla 2 szt. dysków M.2 NVMe umożliwiający montaż dysków i konfigurację ich w systemie RAID 1 na potrzeby instalacji systemu operacyjnego. Montaż tych dysków odbywa się poza standardową przestrzenią na dyski serwera |  |
|  |  | serwer musi być wyposażony w dwa redundantne zasilacze pozwalające na wymianę w trakcie pracy (hot plug) |  |
| 10. | System operacyjny (po jednym do każdego serwera) | Windows Server 2025 Standard (licencja ACADEMIC-EDU) lub równoważny wraz z niezbędnymi licencjami typu Core wynikających z ilości rdzeni zastosowanego procesora (minimum 16) oraz 25 szt. licencji dostępowych User CAL. Warunki równoważności w zakresie sytemu operacyjnego zostały wskazane w dalszej części niniejszego dokumentu. |  |
| 11. | Dokumentacja | dokumentacja użytkownika w języku polskim lub angielskim |  |
| 12. | Dodatkowe elementy wyposażenia | przewody zasilające, szyny montażowe oraz inne akcesoria niezbędne do zamontowania serwera w szafie rack 19’’ |  |
| 13. | Gwarancja | co najmniej 36 miesięcy w miejscu użytkowania, z czasem realizacji następnego dnia roboczego |  |
| 14. | Zgodności z normami | Oferowany serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 oraz musi posiadać deklarację CE |  |
| 15. | Dostęp do oprogramowania | Dostęp do aktualnych sterowników zainstalowanych w serwerze urządzeń, realizowany przez podanie modelu lub nr seryjnego serwera, na dedykowanej przez producenta stronie internetowej. |  |
| 16. | Dodatkowy osprzęt wymagany wraz z dostawą serwera | * 4 szt. - wkładka optyczna SFP Fibre Channel - 10Gbit – kompatybilna z dostarczaną kartą sieciową FP28 * 2 szt. - wkładka optyczna SFP Fibre Channel - 32Gbit – kompatybilna z dostarczaną kartą sieciową FC |  |
| 17. | Dodatkowe okablowanie wymagane wraz z dostawą serwera | * 2 szt. - przewód zasilający o długości minimum 3m C13 – przewód dedykowany do zasilaczy serwerowych * 2 szt. - FC 10Gbit o minimalnej długości 3m – kompatybilne z zamontowaną kartą sieciową - SFP28, * 2 szt. - 32 Gbit o minimalnej długości 3m - kompatybilne z zamontowaną kartą sieciową FC * 7 szt. - patchcord RJ-45 S/FTP kat.6 o minimalnej długości 3m. |  |
| 18. | Stan | Urządzenie nowe, nieużywane, z bieżącej dystrybucji oficjalnego dystrybutora producenta |  |

1. **Macierz dyskowa – 1 sztuka.**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne*** |
| 1. | Obudowa | Do montażu w szafie rack 19’, wysokość maksymalnie 2U |  |
| 2. | Zamontowane dyski | * + 12 szt. – o pojemności co najmniej 2,4 TB (HDD, 10000 obr./min, SAS 12 Gb/s, 2.5″, Hot-Plug),   + 6 szt. – o pojemności co najmniej 1,92 TB (SSD Read Intensive, SAS 24 Gb/s, 2.5″, Hot-Plug). |  |
| 3. | Cechy funkcjonalne | * 1. macierz musi umożliwiać zainstalowanie co najmniej: 24 szt. dysków 2.5" typu SAS, w tym SSD,   2. macierz musi posiadać możliwość rozbudowy pojemności za pomocą dodatkowej półki dyskowej,   3. macierz musi posiadać kontroler FC Type-B 32Gb/s (minimum 2 x 4 porty FC 32Gb/s) wyposażony w minimum 16 GB własnej pamięci cache,   4. macierz musi posiadać interfejs GUI dostępny za pomocą przeglądarki internetowej, pozwalający na konfigurowanie oraz nadzorowanie na prawidłowym funkcjonowaniem macierzy,   5. dodatkowo, macierz musi umożliwiać obsługę za pomocą linii komend (CLI),   6. macierz musi być wyposażona w sprzętowy kontroler dyskowy, umożliwiający konfigurację RAID co najmniej na poziomach: 1, 5, 6, 10.   7. macierz musi być wyposażona w 2 redundantne zasilacze pozwalające na wymianę w trakcie pracy (hot-plug),   8. macierz musi realizować automatyczne przenoszenia danych (auto-tiering) w celu optymalizacji wydajności systemu i efektywności wykorzystania zasobów sprzętowych,   9. macierz musi umożliwiać dynamiczne przydzielanie zasobów pamięci masowej (thin provisioning),   10. macierz musi umożliwiać wykonywanie migawek (snapshots), tworzenie punktów przywracania i zarządzaniu kopiami zapasowymi danych migawek.   11. macierz musi poprawnie współpracować z urządzeniami z następującymi systemami operacyjnymi:       1. Windows Server,       2. Linux,       3. Vmware. |  |
| 4. | Dokumentacja: | W języku polskim lub angielskim |  |
| 5. | Dodatkowe elementy montażowe: | przewody zasilające, szyny montażowe oraz inne akcesoria niezbędne do zamontowania macierzy w szafie rack 19’’. |  |
| 6. | Gwarancja | co najmniej 36 miesięcy w miejscu użytkowania, z czasem realizacji następnego dnia roboczego |  |
| 7. | Normy | produkowana zgodnie z normą ISO-9001:2015 oraz ISO-14001, deklaracja CE. |  |
| 8. | Dodatkowy osprzęt oraz okablowanie | • 8 szt. wkładka optyczna SFP Fibre Channel 32 Gb/s – kompatybilna z kartą sieciową zamontowaną w kontrolerze  • 2 szt. - przewód zasilający o długości minimum 3m C13– przewód dedykowany do zasilaczy zamontowanych w macierzy,  • 4 szt. - patchcord RJ-45 S/FTP kat.6 o minimalnej długości 3m,  • 8 szt. - FC, 32 Gbit o minimalnej długości 3m - kompatybilne z zamontowaną kartą sieciową w macierzy |  |
| 9. | Stan | Urządzenie nowe, nieużywane, z bieżącej dystrybucji oficjalnego dystrybutora producenta |  |

1. **Urządzenie UTM – 1 sztuka.**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne*** |
| 1. | Zastosowanie | Urządzenie typu appliance umożliwiające zapewnienie bezpieczeństwa sieci komputerowej IPv4 i IPv6 przed zagrożeniami z sieci Internet |  |
| 2. | Ilość użytkowników i moduły | Zapewnia bezpieczeństwo dla przynajmniej 50 pracujących użytkowników, przy wykorzystaniu co najmniej następujących modułów:  a) zapobiegania włamaniom (IPS),  b) firewall,  c) kontroli aplikacji,  d) VPN,  e) audytu podatności,  f) systemu antywirusowego,  g) filtra antyspamowego,  h) filtrowania stron internetowych. |  |
| 3. | Licencje | licencje na wskazane powyżej moduły w komplecie z polisą umożliwiającą dokonywanie aktualizacji modułów, baz podatności i zagrożeń, itp. w okresie co najmniej 3 lat od daty dostawy |  |
| 4. | Minimalna wydajność | a) przepustowość firewalla: 4 Gbps,  b) przepustowość IPS: 2 Gbps,  c) ilość tuneli IPSec: 100,  d) ilość jednoczesnych klientów SSL VPN: 50,  e) ilość reguł filtrowania: większa niż 2000. |  |
| 5. | Konfiguracja | możliwość konfiguracji w parze z drugim identycznym urządzeniem w rozwiązanie HA (high availability) w trybie active/passive |  |
| 6. | Interfejsy | Minimum   1. 8 portów Ethernet 100/1000/2500, 2. 1 port światłowodowy 1 Gb. |  |
| 7. | Pamięć logów | Urządzenie musi posiadać gniazdo kart pamięci Micro SD w celu zapisywania logów urządzenia. Wraz z urządzeniem należy dostarczyć kompatybilną kartę o pojemności co najmniej 128 GB. Przekazywanie logów do serwera SYSLOG. |  |
| 8. | Monitoring i podstawowa funkcjonalność | a) zapobieganie włamaniom,  b) wykrywanie i skanowanie automatyczne protokołów,  c) kontrolę aplikacji,  d) ochronę przed atakami: DoS, SQL injection, Cross- Site Scripting (XSS), złośliwym kodem Web2.0 i skryptami  e) wykrywanie trojanów,  f) wykrywanie interaktywnych połączeń tożsamych dla botnetów czy Command & Control,  g) automatyczna kwarantanna w przypadku ataku, działania antyspam i antyphishing,  h) bazę reputacji na podstawie analizy heurystycznej,  i) wbudowane oprogramowanie antywirusowe (HTTP, SMTP, POP3, FTP),  j) deszyfrację i inspekcję ruchu SSL,  k) ochrona VoIP (SIP),  l) dostosowanie polityki filtrowania do zdarzeń bezpieczeństwa,  m) wykrywanie podatności w sieci,  n) wykrywanie niezidentyfikowanych dotychczas zagrożeń przy wykorzystaniu sandboxingu w chmurze. |  |
| 9. | VPN | W zakresie VPN możliwość zestawiania połączeń typu:  a) Site-to-site lub Client-to-site IPSec VPN,  b) Zdalny tunel SSL VPN pomiędzy różnymi systemami operacyjnymi (Windows, Android, iOS),  c) automatycznie konfigurowany klient SSL VPN (Windows), |  |
| 10. | Zarządzanie | Zarządzanie urządzeniem i jego modułami poprzez przeglądarkę internetową, obejmujące co najmniej:  a) zarządzanie politykami,  b) analizę poprawności reguł,  c) skorzystanie z kreatora konfiguracji,  d) globalna / lokalna polityka bezpieczeństwa,  e) raportowanie i prowadzenie analiz,  f) generowanie raportów. |  |
| 11. | Gwarancja | Co najmniej 36 miesięcy |  |
|  | Stan | Urządzenie nowe, nieużywane, z bieżącej dystrybucji oficjalnego dystrybutora producenta |  |

1. **Switch światłowodowy L3 – 1 sztuka.**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne)*** |
| 1. | Zastosowanie | Switch zarządzalny warstwy trzeciej do agregacji łączy o dużej przepustowości z możliwością montażu w szafie rack 19’’ |  |
| 2. | Pojemność przełączania | minimum 700 Gbit/s |  |
| 3. | Minimalne wymagania ilości wbudowanych portów komunikacyjnych | a) 28 portów 10G SFP+,  b) 4 porty 25G SFP28. |  |
| 4. | Zarządzanie | Możliwość zarządzania z poziomu przeglądarki internetowej |  |
| 5. | Gwarancja | Co najmniej 36 miesięcy |  |
| 6. | Dodatkowy osprzęt | • 1 szt. - przewód zasilający C13 o długości minimum 3 m,  • 8 szt. - wkładka optyczna SFP Fibre Channel - 10Gbit,  • 8 szt. - FC 10Gbit o minimalnej długości 3 m,  • uchwyty i śruby montażowe niezbędne do zamontowania w szafie rack 19’’ |  |
| 7. | Stan | Urządzenie nowe, nieużywane, z bieżącej dystrybucji oficjalnego dystrybutora producenta |  |

1. **Switch ethernetowy – 2 sztuka.**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne*** |
| 1. | Zastosowanie | Switch zarządzalny warstwy trzeciej z możliwością montażu w szafie rack 19’’ |  |
| 2. | Pojemność przełączania | minimum 200 Gbit/s |  |
| 3. | Minimalne wymagania ilości wbudowanych portów komunikacyjnych | * 16 portów RJ45 2,5 GbE, * 32 porty RJ45 GbE, * 4 porty 10G SFP+. |  |
| 4. | Zarządzanie | Możliwość zarządzania z poziomu przeglądarki internetowej |  |
| 5. | Gwarancja | Co najmniej 36 miesięcy |  |
| 6. | Dodatkowy osprzęt | * 1 szt. - przewód zasilający C13 o długości minimum 3 m, * 4 szt. - wkładka optyczna SFP Fibre Channel - 10Gbit, * 4 szt. - FC 10Gbit o minimalnej długości 3 m, * 12 szt. - patchcord RJ-45 S/FTP kat.6 o minimalnej długości 3 m, * 6 szt. - patchcord RJ-45 S/FTP kat.6 o minimalnej długości 5 m, * 6 szt. - patchcord RJ-45 S/FTP kat.6 o minimalnej długości 1 m, * uchwyty i śruby montażowe niezbędne do zamontowania w szafie rack 19’’. |  |
| 7. | Stan | Urządzenie nowe, nieużywane, z bieżącej dystrybucji oficjalnego dystrybutora producenta |  |

1. **Szafa rack 19’’ wraz z akcesoriami – 1 sztuka.**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne*** |
| 1. | Zastosowanie | szafa rack 19’’ typu open rack. |  |
| 2. | Wymiary | * + Wysokość 32 U   + Szerokość maks. 60 cm   + Głębokość minimum 100cm   + Ładowność co najmniej 600kg   + Zakres regulowanej głębokości montażowej: 550-790mm |  |
| 3. | kolor | * czarny |  |
| 4. | Elementy wyposażenia | a) kółka z hamulcem, nóżki, śruby M6.  b) 4 szt. - półka z otworami 350mm 1U, 19" do szafy RACK (kolor czarny)  c) 2 szt. - półka stała 19", 1U, gł. 750mm, mont. przód/tył, regulowana w zakresie: 750-900mm (kolor czarny)  d) 4 szt. - organizator kabli poziomy 19" 1U do szafy RACK (kolor czarny)  e) 4 szt. - zaślepka 19" 1U do szafy RACK (kolor czarny)  f) 2 szt. - listwa zasilająca 230V do szafy rack 19", 9 gniazd z wyłącznikiem, 3 m, (9 standardowych gniazd typu NFC61-314 oraz wtyk DIN 49441 standard stosowany w Polsce) wtyczka UPS C14  g) 10 szt. - zestaw montażowy RACK M6 (śruba + koszyczek + podkładka), (kolor czarny) |  |
| 5. | Gwarancja | Co najmniej 36 miesięcy |  |
| 6. | Stan | Urządzenie nowe, nieużywane. |  |

1. **UPS do szafy rack 19’’– 1 sztuka.**

Producent ……………………………..

Model ……………………………..

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Parametr** | **Charakterystyka** | **Potwierdzenie spełnienia wymagania**  **(należy potwierdzić) *(wpisać szczególnie w miejscach, gdzie określono zakresy lub wartości minimalne/maksymalne*** |
| 1. | Zastosowanie | UPS do montażu i zasilania awaryjnego urządzeń montowanych w szafie rack 19’’ |  |
| 2. | Moc | * + Czynna (realna) – 3000W   + Pozorna - 3000 VA |  |
| 3. | Typ | UPS online (VFI) |  |
| 4. | Postać napięcia wyjściowego | czysta sinusoida |  |
| 5. | Gniazda wyjściowe | minimum 8 × IEC C13 |  |
| 6. | Złącza komunikacyjne | USB, RS-232, RJ-45, SNMP slot |  |
| 7. | Czas podtrzymywania | nie więcej niż 6 godzin do 90%. |  |
| 8. | El. panelu | Wyświetlacz LCD: wskazujący napięcie, obciążenie, czas pracy, stan baterii |  |
| 9. | Wysokość | Maksymalnie 3U |  |
| 10. | Montaż | dołączone uszy montażowe + opcjonalne szyny prowadzące |  |
| 11. | Gwarancja | Co najmniej 36 miesięcy |  |
| 12. | Stan | Urządzenie nowe, nieużywane. |  |

**Wymagania wspólne dla dostarczanych urządzeń:**

1. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający zastrzega sobie prawo do żądania od Wykonawcy dokumentów potwierdzających, że oferowany sprzęt pochodzi z autoryzowanego kanału dystrybucji.
2. Wszystkie elementy oferowanego urządzenia muszą być jego integralną części (Zamawiający nie akceptuje kart sieciowych, dysków twardych podłączanych za pomocą złączy zewnętrznych USB, eSATA, ExpressCard).

**Parametry równoważności dla systemów operacyjnych:**

1. **Windows 11 Professional PL**
2. Licencja systemu operacyjnego typu wieczystego.
3. System operacyjny przeznaczony dla komputerów przenośnych, z graficznym interfejsem użytkownika.
4. System operacyjny musi pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016; MS Office 365.
5. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
   1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
6. Interfejsy użytkownika muszą być dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
7. Zlokalizowane w języku polskim, muszą być co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.
8. System operacyjny musi posiadać wbudowany system pomocy w języku polskim.
9. Graficzne środowisko instalacji i konfiguracji musi być dostępne w języku polskim.
10. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu operacyjnego z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z dostępnych poprawek są potrzebne w konkretnej wersji systemu operacyjnego.
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu informatycznego wykorzystywanego aktualnie przez Zamawiającego.
12. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
13. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych oraz zintegrowana z systemem, konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
14. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
15. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
16. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
17. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę należy rozumieć zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
18. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
19. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
20. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników muszą być zarządzane zdalnie; praca systemu operacyjnego w trybie ochrony kont użytkowników.
21. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:
    1. poziom menu,
    2. poziom otwartego okna systemu operacyjnego,
    3. system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
23. Obsługa standardu NFC (near field communication).
24. Możliwość przystosowania stanowiska komputerowego pod kontrolą systemu operacyjnego dla osób z niepełnosprawnościami (np. słabo widzących);
25. Wsparcie dla protokołu IPSEC oparte na politykach – wdrażanie IPSEC musi być oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
26. Mechanizmy logowania do domeny w oparciu o:
    1. Login i hasło,
    2. Karty z certyfikatami (smartcard),
    3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
27. Mechanizmy wieloelementowego uwierzytelniania.
28. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.
29. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPSEC.
30. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
31. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
32. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
33. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem wsparcia bieżącego użytkownika komputera.
34. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie to musi umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację.
35. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
36. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
37. Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
38. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
39. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
40. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
41. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie co najmniej 4 maszyn wirtualnych.
42. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego tylko do danych użytkownika.
43. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
44. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
45. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
46. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu operacyjnego.
47. **Windows Server 2025 Standard**
48. Oferowane równoważne rozwiązanie musi być zainstalowane bezpośrednio na sprzęcie fizycznym - nie może być częścią innego systemu operacyjnego.
49. Oferowane równoważne rozwiązanie musi uprawniać do instalacji\uruchomienia środowisk gości działających pod kontrolą systemu operacyjnego z rodziny MS Windows.
50. Oferowane równoważne rozwiązanie ma pełnić rolę narzędzia pozwalającego na migrację maszyn wirtualnych klientów działających na Hyper-V oraz serwerach fizycznych z systemami MS Windows.
51. Pozwalać na wykorzystanie odpowiedniej liczby rdzeni logicznych procesorów oraz pamięci RAM oferowanych serwerów fizycznych.
52. Pozwalać na wykorzystywania procesorów wirtualnych oraz pamięci RAM i dysku przez gościa.
53. Zapewniać możliwość dodawania zasobów w czasie pracy gościa, w szczególności w zakresie ilości procesorów, pamięci operacyjnej, przestrzeni dyskowej, interfejsów sieciowych.
54. Posiadać centralny mechanizm monitorowania i zarządzania dostępem gości do przestrzeni dyskowej będący odpowiednikiem „Storage Quality of Service”.
55. Posiadać mechanizm zarządzania przestrzeniami dyskowymi będący odpowiednikiem „Storage Spaces Direct” (S2D).
56. Posiadać mechanizm replikacji przestrzeni dyskowych będący odpowiednikiem „Storage Replica”:
    1. działający zarówno w trybie server-to-server, jak i cluster-to-cluster,
    2. wspierający replikację synchroniczną i asynchroniczną.
57. Posiadać funkcjonalności przełącznika.
    1. Zarządzanie pasmem (np. za pomocą techniki „traffic shaping”),
    2. Zabezpieczenie przed niepożądanym działaniem gości,
    3. Zabezpieczenie przed “Neighbor Discovery Poisoning”,
    4. Wsparcie dla DHCP,
    5. Kontrolę dostępu na poziomie portów sieciowych,
    6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode),
    7. Monitorowanie ruchu sieciowego,
    8. Izolowanie ruchu w ramach wybranych grup gości separujących ruch wymieniany pomiędzy nimi (odpowiednik isolated\private LAN).
58. Posiadać możliwość budowania klastrów niezawodnościowych składających się z maksymalnie 64 węzłów (odpowiednik funkcjonalności Failover Clusters).
59. Posiadać możliwość federowania klastrów typu niezawodnościowego (Failover Clusters) w zespół klastrów z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu (odpowiednik funkcjonalności Cluster Set).
60. Posiadać wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny.
61. Posiadać odpowiednik rozwiązania „Shielded VM”, czyli możliwość szyfrowania obrazów gości (również podczas migracji), stanu gości oraz ograniczenie możliwości ich uruchomienia wyłącznie do przypadku, gdy są na liście zweryfikowanych obrazów oparty o TPM 2.0.
62. Posiadać możliwość narzucania 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.
63. Posiadać możliwość automatycznej aktualizacji w modelu „rolling update”:
    1. w oparciu o poprawki publikowane przez producenta w sieci Internet,
    2. z możliwością lokalnej dystrybucji poprawek zatwierdzonych przez administratora rozwiązania, bez połączenia z siecią Internet