**Załącznik nr 6 do SIWZ**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Zakres zamówienia obejmuje wykonanie serwerowni w pomieszczeniu centralnego magazynu zbiorów muzealnych Muzeum Rolnictwa w Ciechanowcu oraz dostarczenie systemu, na który składa się: infrastruktura IT i oprogramowanie.

Na całość systemu składają się następujące komponenty:

 • Infrastruktura IT:

- Dostarczenie i wyposażenie szafy serwerowej,

- Infrastruktura serwerowa na potrzeby podsystemów oprogramowania,

- Infrastruktura na potrzeby przechowywania danych,

 • Oprogramowanie:

- Platforma wirtualizacyjna

- Systemy operacyjne hostów,

- Serwisy umożliwiające prowadzenie usług WEB

- Serwisy dostarczające zabezpieczenie usługi DNS

- System autoryzacji użytkowników

Na podstawie powyższej infrastruktury zamawiający planuje realizować niżej opisane usługi. Oferowane rozwiązanie musi zapewnić sprawną realizację niżej opisanych usług.

Usługi platformy wirtualizacyjnej:

Stworzenie solidnego i stabilnego rozwiązania bazującego na doświadczeniu i najlepszych obecnych praktykach zapewniającego infrastrukturę o wysokiej dostępności (High Availability) oraz skalowalności, pozwalające
na elastyczne uruchomienie i świadczenie potrzebnych usług. Zapewniające niezależność od warstwy sprzętowej
- system powinien zostać wdrożony i zoptymalizowany pod kątem zapewnienia wysokiej wydajności we współpracy
ze sprzętem zaproponowanym przez Wykonawcę

Usługi maszyn wirtualnych:

Możliwość tworzenia i uruchamiania w ramach klastra maszyn wirtualnych z różnymi dostępnymi na rynku systemami operacyjnymi w roli hosta, które umożliwiają optymalne wykorzystanie infrastruktury. Poszczególne tworzone maszyny wirtualne powinny umożliwiać:

 • Możliwość samodzielnej konfiguracji wirtualnego serwera oraz instalacji oprogramowania

 • Zarządzanie wirtualnym serwerem przez panel administracyjny,

 • Skalowalność wirtualnego serwera (zmiana parametrów w panelu lub przez API),

 • Zarządzanie oraz monitoring serwerów wirtualnych,

Firewall/UTM z obsługą VPN:

W celu zapewnienia wysokiego poziomu bezpieczeństwa wymagane jest dostarczenie i wdrożenie rozwiązania zabezpieczającego komunikację z serwerami i tradycyjnymi komputerami oraz urządzeniami mobilnymi umożliwiające bezpieczny dostęp tylko dla uprawnionych użytkowników w oparciu o technologię wirtualnych sieci prywatnych. Zaoferowane rozwiązanie powinno zapewniać sprzętowe wsparcie dla realizowanych połączeń i odbywać się poprzez dostarczoną zaporę sieciową klasy UTM. Rozwiązanie powinno gwarantować:

 • Prostą instalację i konfigurację,

 • Brak konieczności zarządzania sprzętem przez użytkowników,

 • Niezależność klientów (oprogramowania klienckiego) od systemu operacyjnego,

 • Obsługa urządzeń mobilnych,

W ramach Projektu Wykonawca musi dostarczyć, skonfigurować, zintegrować i wdrożyć zaoferowany sprzęt, oprogramowanie oraz przeprowadzić wszelkie czynności niezbędne do produkcyjnego uruchomienia dostarczonego rozwiązania i rozpoczęcia świadczenia Usług przez Zamawiającego.

1. **Serwer - 2 szt.**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3,5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowane dwa procesory ośmiordzeniowe x86 min. 2,1 GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 13 100 w teście CPU Benchmark dostępnym na stronie www.cpubenchmark.net  |
| **RAM** | 128 GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 8 wolnych slotów przeznaczonych do rozbudowy pamięci. Płyta główna powinna obsługiwać do min. 1 TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling |
| **Gniazda PCI** | Min. 2 sloty generacji 3 o prędkości x8  |
| **Interfejsy sieciowe** | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz zainstalowane dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+ wraz z kompatybilnymi wkładkami ze złączami LC. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.- cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.- cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT. |
| **Karta HBA** | Zainstalowana karta HBA umożliwiająca połączenie z macierzą po protokole Fibre Channel, wyposażona w dwa porty o prędkości minimum 8Gb |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD, NVMe. Zainstalowane dyski:2 dyski o pojemności 480GB SSD HotPlug 6Gb/s Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |
| **Napęd optyczny** | Serwer musi być wyposażony w napęd optyczny DVD +/- RW. Napęd musi być integralną częścią zamawianego serwera, nie dopuszcza się napędów podłączanych poprzez port USB. |
| **Wbudowane porty** | 3xUSB, min.1 port USB 2.0 oraz 3 porty USB 3.0, min. 1 port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug, minimum 550 W każdy. |
| **Bezpieczeństwo** | Zintegrowany z płytą główną moduł TPM.Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **Diagnostyka** | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Oprogramowanie** | System Windows 2019 Standard lub równoważny dostarczony z niezbędnymi licencjami pozwalającymi na uruchomienie 8 maszyn wirtualnych oraz 50 CALi dla użytkowników. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
* karta z możliwością wyposażenia we wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.

Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:* wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
* możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
* wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
* możliwość oskryptowywania procesu wykrywania urządzeń;
* możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
* szczegółowy opis wykrytych systemów oraz ich komponentów;
* możliwość eksportu raportu do CSV, HTML, XLS;
* grupowanie urządzeń w oparciu o kryteria użytkownika;
* automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
* szybki podgląd stanu środowiska;
* podsumowanie stanu dla każdego urządzenia;
* szczegółowy status urządzenia/elementu/komponentu;
* generowanie alertów przy zmianie stanu urządzenia;
* filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
* integracja z service desk producenta dostarczonej platformy sprzętowej;
* możliwość przejęcia zdalnego pulpitu;
* możliwość podmontowania wirtualnego napędu;
* kreator umożliwiający dostosowanie akcji dla wybranych alertów;
* możliwość importu plików MIB;
* przesyłanie alertów „as-is” do innych konsol firm trzecich;
* aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
* możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
* możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
* moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
 |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2 x64, Microsoft Windows Server 2016, Microsoft Windows Server 2019. |
| **Warunki gwarancji** | Gwarancja realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 9/5 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii nośników pozostają one własnością Zamawiającego.Zamawiający wymaga, aby firma serwisująca posiadała ISO 9001:2008 na świadczenie usług serwisowych oraz posiadała autoryzacje producenta urządzeń. – dokumenty potwierdzające należy załączyć przed podpisaniem umowy.Wymagane dołączenie (przed podpisaniem umowy) oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.* Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
* Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu.

W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

1. **Macierz – 1 szt.**

|  |  |
| --- | --- |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5”. Dołączone szyny montażowe do szafy RACK 19” |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów w tym minimum 4 porty w standardzie FC wraz z 4 wkładkami FC 16 Gb oraz 4 portami ISCSI 10Gb SFP+ |
| **Cache** | 8GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. |
| **Dyski**  | Zainstalowanych łącznie 24 dysków Hot-Plug SAS o pojemności 2,4TB SAS 10k RPM 2,5”, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| **Zasilacze** | Zainstalowane dwa redundantne zasilacze o mocy minimum 570W umożliwiające wymianę bez wyłączania macierzy. |
| **Oprogramowanie/Funkcjonalności** | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| **Wsparcie dla systemów operacyjnych** | Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi. |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| **Warunki gwarancji dla macierzy** | Gwarancja realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 9/5 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii nośników pozostają one własnością Zamawiającego.Zamawiający wymaga, aby firma serwisująca posiadała ISO 9001:2008 na świadczenie usług serwisowych oraz posiadała autoryzacje producenta urządzeń. – dokumenty potwierdzające należy załączyć przed podpisaniem umowy.Wymagane dołączenie (przed podpisaniem umowy) oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.* Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
* Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu.
* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Certyfikaty** | Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2008.  |

1. **Półka dyskowa do macierzy – 1 szt.**

|  |  |
| --- | --- |
| **Parameter** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19”, półka musi zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5”. Półka musi być kompatybilna i umożliwiać połączenie z macierzą zaproponowaną w punkcie 1.Półka musi być dostarczona wraz z kompletem kabli umożlwiających podłączenie z macierzą. |
| **Dyski**  | Zainstalowanych łącznie 6 dysków Hot-Plug SATA o pojemności 8TB 7.2k RPM 3,5” oraz 6 dysków 960GB SSD 2,5” w ramce 3,5”. |
| **Wsparcie dla systemów operacyjnych** | Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi. |
| **Warunki gwarancji dla macierzy** | Gwarancja realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 9/5 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii nośników pozostają one własnością Zamawiającego.Zamawiający wymaga, aby firma serwisująca posiadała ISO 9001:2008 na świadczenie usług serwisowych oraz posiadała autoryzacje producenta urządzeń. – dokumenty potwierdzające należy załączyć przed podpisaniem umowy.Wymagane dołączenie (przed podpisaniem umowy) oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.* Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
* Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu.
* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Certyfikaty** | Półka dyskowa musi być wyprodukowany zgodnie z normą ISO 9001:2008.  |

**4. Przełącznik sieciowy – 2szt.**

|  |  |
| --- | --- |
| **Obudowa** | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U. |
| **Porty** | Minimum 48 portów 1GbE PoE+. Minimum 2 porty 10Gb SFP+ oraz 2 porty SFP (combo) |
| **Wydajność** | obsługa minimum 200 wirtualnych sieci |
| Przepustowość minimum 328Gbps w trybie full-duplex, Wielkość tablicy MAC minimum 32000, rozmiar bufora pakietów minimum 4MB, 8 kolejek na port |
| **Zgodność z protokołami** | IEEE 802.1D Spanning Tree, GARP i GVRP |
| IEEE 802.1p Traffic Prioritization |
| IEEE 802.1Q VLAN Trunking |
| IEEE 802.1w Rapid Spanning Tree Protocol |
| IEEE 802.1S Multiple Spanning Tree Protocol |
| IEEE 802.1t IEEE802.1D maintenance |
| IEEE 802.1v VLAN Classification by Protocol & Port |
| IEEE 802.1x Port Based Network Access Control |
| IEEE 802.3 10 Mbps Ethernet |
| IEEE 802.3I 10base -T |
| IEEE 802.3u 100Base-T Ethernet |
| IEEE 802.3z 1000 Mbps Ethernet |
| IEEE 802.3ab 1000Base-T |
| IEEE 802.3ac Frame extension for VLAN tags |
| IEEE 802.3ad Link Aggregation Control Protocol |
| IEEE 802.3ae 10 Gig Ethernet |
| IEEE 802.2  |
| IEEE 802.3x Flow Control |
| IEEE 802.3I |
| IEEE 802.1v VLAN Classification by Protocol & Port |
| IEEE 802.1ab LLDP |
| ANSI/TIA-1057-2006 LLDP-MEDW |
|   |
| **Zarządzanie siecią i bezpieczeństwo** | HTTP Over TLS |
| Radius |
| Radius Accounting |
| RADIUS Tunnel Authentication |
| DHCP options oraz BOOTP vendor extensions |
| Dynamic Host Configuration Protocol (DHCP) klient |
| Bootstrap Protocol |
| DNS Client |
| Form-based File Upload in HTML |
| Simple Network Time Protocol (SNTP) |
| Wsparcie dla IPv6 |
| IGMPv2 snooping |
| MLD Snooping |
| TLS protocol, version 1.0 |
| PPP Extensible Authentication Protocol, EAP |
| Hypertext Transfer Protocol -- HTTP/1.1 |
| BSD Syslog Protocol |
| IGMPv3 snooping |
| SNMP v1 v2 |
| RMON |
| Simple Network Time Protocol (SNTP) Version 4 dla IPv4, IPv6  |
| Port, VLAN mirroring |
| DHCP Server |
| Wsparcie dla ramek typu Jumbo  9,000 bajtów |
| Broadcast storm control |
| Możliwość wgrywania oprogramowania przez USB |
| Zarządzanie za pomocą graficznej konsoli WEB |
| Trivial File Transfer Protocol (TFTP) Rev. 2 |
| Wsparcie dla agregacji LACP (802.3ad) - minimum 12 grup do 4 portów na grupę |
| Honorowanie wartości 802.1p oraz IP DSCP  |
| Wsparcie kolejkowania Strict priority oraz algorytmu weighted round robin (WRR) |
| wsparcie dla VLAN ID w ilości 4096  |
| Private VLAN |
| Guest VLAN |
| Voice/Multicast TV VLAN |
| Locked Port |
| dostępne profile konfiguracji portów |
| **Certyfikaty i standardy** | Zamawiający wymaga aby oferowany przełącznik: |
| - został wyprodukowany zgodnie z normą  ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) |
| - posiadał deklarację CE (dokument załączyć do oferty) |
| - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta załączyć do oferty) |

**5.** **Przełącznik sieciowy – 3 szt.**

|  |  |
| --- | --- |
| **Obudowa** | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U. |
| **Porty** | Minimum 24 porty 1GbE. Minimum 4 porty 10Gb SFP+  |
| **Wydajność** | obsługa minimum 200 wirtualnych sieci |
| Przepustowość minimum 128Gbps w trybie full-duplex, Wielkość tablicy MAC minimum 16000, rozmiar bufora pakietów minimum 1MB, 8 kolejek na port |
| **Zgodność z protokołami** | IEEE 802.1D Spanning Tree, GARP i GVRP |
| IEEE 802.1p Traffic Prioritization |
| IEEE 802.1Q VLAN Trunking |
| IEEE 802.1w Rapid Spanning Tree Protocol |
| IEEE 802.1S Multiple Spanning Tree Protocol |
| IEEE 802.1t IEEE802.1D maintenance |
| IEEE 802.1v VLAN Classification by Protocol & Port |
| IEEE 802.1x Port Based Network Access Control |
| IEEE 802.3 10 Mbps Ethernet |
| IEEE 802.3I 10base -T |
| IEEE 802.3u 100Base-T Ethernet |
| IEEE 802.3z 1000 Mbps Ethernet |
| IEEE 802.3ab 1000Base-T |
| IEEE 802.3ac Frame extension for VLAN tags |
| IEEE 802.3ad Link Aggregation Control Protocol |
| IEEE 802.3ae 10 Gig Ethernet |
| IEEE 802.2  |
| IEEE 802.3x Flow Control |
| IEEE 802.3I |
| IEEE 802.1v VLAN Classification by Protocol & Port |
| IEEE 802.1ab LLDP |
| ANSI/TIA-1057-2006 LLDP-MEDW |
| **Zarządzanie siecią i bezpieczeństwo** | HTTP Over TLS |
| Radius |
| Radius Accounting |
| RADIUS Tunnel Authentication |
| DHCP options oraz BOOTP vendor extensions |
| Dynamic Host Configuration Protocol (DHCP) klient |
| Bootstrap Protocol |
| DNS Client |
| Form-based File Upload in HTML |
| Simple Network Time Protocol (SNTP) |
| Wsparcie dla IPv6 |
| IGMPv2 snooping |
| MLD Snooping |
| TLS protocol, version 1.0 |
| PPP Extensible Authentication Protocol, EAP |
| Hypertext Transfer Protocol -- HTTP/1.1 |
| BSD Syslog Protocol |
| IGMPv3 snooping |
| SNMP v1 v2 |
| RMON |
| Simple Network Time Protocol (SNTP) Version 4 dla IPv4, IPv6  |
| Port, VLAN mirroring |
| DHCP Server |
| Wsparcie dla ramek typu Jumbo  9,000 bajtów |
| Broadcast storm control |
| Możliwość wgrywania oprogramowania przez USB |
| Zarządzanie za pomocą graficznej konsoli WEB |
| Trivial File Transfer Protocol (TFTP) Rev. 2 |
| Wsparcie dla agregacji LACP (802.3ad) - minimum 12 grup do 4 portów na grupę |
| Honorowanie wartości 802.1p oraz IP DSCP  |
| Wsparcie kolejkowania Strict priority oraz algorytmu weighted round robin (WRR) |
| wsparcie dla VLAN ID w ilości 4096  |
| Private VLAN |
| Guest VLAN |
| Voice/Multicast TV VLAN |
| Locked Port |
| dostępne profile konfiguracji portów |
| **Certyfikaty i standardy** | Zamawiający wymaga aby oferowany przełącznik: |
| - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty) |
| - posiadał deklarację CE (dokument załączyć do oferty) |
| - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta załączyć do oferty) |

**6. Zabezpieczenie klasy UTM**

# **Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
* 20 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP 1 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.
4. System musi być wyposażony w zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps.

# **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

# **Polityki, Firewall**

1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

# **Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

# **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

# **Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

# **Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

# **Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

# **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

# **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

# **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

# **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

# **Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

# **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.
* ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
* ICSA dla funkcji SSL VPN.

# **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 12 miesięcy.

# **Gwarancja oraz wsparcie**

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# **Opisy do wymagań ogólnych**

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**7. Access Point – 5 szt.**

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
	1. Temperatura -20–50°C,
	2. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
	1. 2.4 GHz 802.11b/g/n,
	2. 5 GHz 802.11a/n/ac,
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Liczba interfejsów:
	1. Ethernet – 1 w standardzie 10/100/1000 Base-TX,
	2. USB – 1 Typ A.
6. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
	1. Tunnel,
	2. Bridge,
	3. Mesh.
8. Wsparcie dla QoS: 802.11e, WME/WMM Multimedia Extensions, konfigurowalne polityki QoS per użytkownik/aplikacja.
9. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
	1. MIMO – 2x2,
	2. Transmit Beam Forming (TxBF),
	3. Maksymalna przepustowość dla poszczególnych modułów radiowych:
		1. 400 Mbps;
		2. 867 Mbps;
	4. Wymagana moc nadawania:
		1. min. 25 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
		2. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
	5. Wsparcie dla 802.11n 20/40Mhz HT,
	6. Wsparcie dla kanału 80 MHz dla 802.11ac,
	7. Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
	8. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
	9. Maksymalna deklarowana liczba klientów per moduł radiowy – 512.
11. Funkcje interfejsu radiowego:
	1. Skaner częstotliwości 2.4 oraz 5 GHz,
	2. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
	3. Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,
12. Funkcje dodatkowe:
	1. Low-Density Parity Check (LDPC) Encoding,
	2. Maximum Likelihood Demodulation (MLD),
	3. Maximum Ratio Combining (MRC),
	4. A-MPDU and A-MSDU Packet Aggregation,
	5. MIMO Power Save,
	6. Short Guard Interval,
	7. WME Multimedia Extensions.
13. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

**8. Oprogramowanie do backupu komputerów stacjonarnych i maszyn wirtualnych z dwóch serwerów z pkt 1.**

 **8.1 Oprogramowanie do backupu komputerów stacjonarnych**

* Rozwiązanie musi wykonywać kopię zapasową systemu Windows wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
* Rozwiązanie musi być licencjonowane subskrypcyjnie, per agent, łącznie na 5 lat
* Rozwiązanie musi wspierać Windows 7 SP1, lub nowsze oraz Windows Server 2008 R2 SP1 lub nowsze
* Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
	+ NTFS
	+ ReFS
	+ FAT32
* Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
* 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:
	+ 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.
	+ Zcentralizowanym repozytorium danych
	+ Bezpośrednio na zasobach Chmury
	+ Microsoft OneDrive/OneDrive for Business
* Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
* Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych
* Rozwiązanie musi wspierać technologię BitLocker
* Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. Nośnik odtwarzania musi być automatycznie tworzony przez Rozwiązanie
* Rozwiązanie musi wspierać wgrywanie dodatkowych sterowników podczas odtwarzania z wykorzystaniem nośnika odtwarzania
* Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
	+ Microsoft Exchange 2010 i nowszych
	+ Microsoft Active Directory 2003 i nowszych
	+ Microsoft Sharepoint 2010 i nowszych
	+ Microsoft SQL 2005 i nowszych
	+ Oracle for Windows 11g i nowszych
* Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
* Rozwiązanie musi wspierać szyfrowanie
* Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
* Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
* Rozwiązanie musi posiadać funkcjonalność ochrony przed ransomware dla nośników wymiennych wykorzystywanych, jako repozytorium kopii zapasowych
* Rozwiązanie musi wspierać tworzenie kopii zapasowych wykorzystując konsolę tekstową lub CLI
na maszynie zabezpieczanej
* Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
* Oprogramowanie do backupu komputerów stacjonarnych musi posiadać wspólną konsolę zarządzania wraz
z oprogramowaniem do backupu serwerów wirtualnych

**8.2 Oprogramowanie do backupu maszyn wirtualnych z dwóch serwerów z pkt. 1.**

# **Wymagania ogólne**

* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
* W oprogramowaniu do backupu dla serwerów wymagana jest licencja wieczysta z rocznym dostępem
do aktualizacji oprogramowania, poprawek oraz wsparciem supportu producenta
* Oprogramowanie do backupu serwerów wirtualnych musi posiadać wspólną konsolę zarządzania wraz
z oprogramowaniem do backupu komputerów stacjonarnych

# **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 musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.
* Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
* 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.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
* Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX
na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

# **Wymagania RPO**

* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* 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 na wszystkich wspieranych platformach wirtualizacyjnych
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
* Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
* Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019
z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

# **Wymagania RTO**

* Oprogramowanie musi umożliwiać 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 niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
* 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 umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
1. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	1. **Linux**
		1. ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
	2. **BSD**
		1. UFS, UFS2
	3. **Solaris**
		1. ZFS, UFS
	4. **Mac**
		1. HFS, HFS+
	5. **Windows**
		1. NTFS, FAT, FAT32, ReFS
	6. **Novell OES**
		1. NSS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
* 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.
* Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
* Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
* Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

# **Ograniczenie ryzyka**

* Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere
i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
* 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
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
* 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.
* Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych
z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

# **Monitoring**

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio
z narzędzia monitorującego
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* 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.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x

# **Raportowanie**

* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.x vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich
do odbiorców w określonych przez administratora interwałach
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje
z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian
w celu optymalnego wykorzystania fizycznej infrastruktury
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania
do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego
na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje
z dowolnych predefiniowanych raportów w pojedynczym dokumencie

**9. Szafa RACK**

|  |  |
| --- | --- |
| **Szafa RACK** | Maksymalna wysokość: 206cmMaksymalna szerokość: 80.0cmMaksymalna głębokość: 106.0cmWysokość w szafie: 42UCiężar netto 131kgMaksymalna głębokość montażu: 77.72cmMinimalna głębokość montażu: 16.76cmSzerokość szafy: 19"Klasa ochrony: IP 20Certyfikaty i zgodność z normami: UL 2416, UL 60950-1Gwarancja: - naprawa lub wymiana 5 latMożliwość zdejmowania paneli bocznychPerforowane drzwi przednie oraz tylneKółka samonastawne – 4szt.Póki: 2szt |

**10. Wdrożenie**

Zamawiający wymaga następujących czynności wchodzących w skład wdrożenia:

1. Montaż wszystkich urządzeń w szafie RACK
2. Demontaż wszystkich zbędnych urządzeń wchodzących w skład aktualnej infrastruktury IT
3. Montaż Access Pointów we wskazanych przez zamawiającego miejscach
4. Wdrożenie domeny oraz GPO wraz z polityką haseł między innymi z następującymi zasadami grupy:
5. Hasło musi spełniać wymagania co do złożoności
6. Minimalny okres ważności hasła
7. Wymuszaj tworzenie historii haseł
8. Maksymalny okres ważności hasła
9. Minimalna długość hasła
10. Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego
11. Próg blokady konta
12. Czas trwania blokady
13. Wyzeruj liczniki blokady konta po
14. Logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika
15. Logowanie interakcyjne: nie wymagaj naciśnięcia klawiszy CTRL+ALT+DEL
16. Logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować
17. Logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować
18. Logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem
19. Zamknięcie: zezwalaj na zamykanie systemu bez konieczności załogowania
20. Logowanie lokalne
21. Odmowa logowania lokalnego
22. Uzyskiwanie dostępu do tego komputera z sieci
23. Odmowa dostępu do tego komputera z sieci
24. Usuń Menedżera zadań
25. Usuń opcję zablokuj komputer
26. Usuń opcję Zmień hasło
27. Usuń wylosowywanie
28. Wdrożenie serwera WWW
29. Wdrożenie serwera plików
30. Przeniesienie oprogramowania RAKS do nowej serwerowni
31. Konfiguracja środowiska do wirtualizacji oraz uruchomienie wybranych maszyn wirtualnych
32. Konfiguracja nowej sieci dla serwerowni oraz 3 odrębnych lokalizacji, wraz z punktami dostępowymi WiFi.
33. Segmentacja sieci poprzez utworzenie odpowiednich VLAN-ów
34. Instalacja i konfiguracja oprogramowania do backupu wraz z utworzeniem polityk retencji, harmonogramów oraz wydzieleniem segmentu sieci dedykowanemu tylko pod przesyłanie backupu
35. Konfiguracja dodatkowego backupu danych o znaczeniu krytycznym na posiadane przez zamawiającego urządzenie Qnap TS-431P
36. Napisanie wszystkich niezbędnych skryptów backupowych koniecznych wskazanych przez zamawiającego
37. Wszelkie okablowanie, wkładki 10Gb SFP+ i inne media wymaganie do połączeń między urządzeniami mają zostać dostarczone przez wykonawcę