Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

**SPIS TREŚCI**

[**Wstęp 3**](#_heading=h.gjdgxs)

[**Wymagania minimalne 4**](#_heading=h.30j0zll)

[Część I przedmiotu zamówienia 4](#_heading=h.1fob9te)

[Serwer z oprogramowaniem systemowym wraz ze szkoleniem i wdrożeniem 4](#_heading=h.3znysh7)

[Część II przedmiotu zamówienia 7](#_heading=h.2et92p0)

[Przełączniki sieciowe wraz ze szkoleniem 7](#_heading=h.tyjcwt)

[Część III przedmiotu zamówienia 10](#_heading=h.3dy6vkm)

[Oprogramowanie do szyfrowania poczty wraz ze szkoleniem 10](#_heading=h.1t3h5sf)

[Część IV przedmiotu zamówienia 12](#_heading=h.4d34og8)

[UPS 12](#_heading=h.2s8eyo1)

[Część V przedmiotu zamówienia 13](#_heading=h.17dp8vu)

[Urządzenie do backupu - typ I 13](#_heading=h.3rdcrjn)

[Urządzenie do backupu - typ II 14](#_heading=h.lnxbz9)

[Część VI przedmiotu zamówienia 16](#_heading=h.35nkun2)

[Stacje robocze 16](#_heading=h.1ksv4uv)

[Część VII przedmiotu zamówienia 22](#_heading=h.44sinio)

[Urządzenie klasy UTM 22](#_heading=h.2jxsxqh)

[Część VIII przedmiotu zamówienia 25](#_heading=h.z337ya)

[Audyt bezpieczeństwa- część II przedmiotu zamówienia 25](#_heading=h.3j2qqm3)

[Część IX przedmiotu zamówienia 26](#_heading=h.1y810tw)

[Szkolenia dla pracowników z zakresu cyberbezpieczeństwa 26](#_heading=h.4i7ojhp)

[**Wymagania dodatkowe 27**](#_heading=h.2xcytpi)

# **Wstęp**

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowa Gmina” realizowanego przez Gminę Ząbkowice Śląskie.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina” dla Gminy Ząbkowice Śląskie o numerze 2983/1/2021.

# **Wymagania minimalne**

## Część I przedmiotu zamówienia

## Serwer z oprogramowaniem systemowym wraz ze szkoleniem i wdrożeniem

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zamawiający wymaga dostarczenia w ramach dostawy:  1 kpl. serwer domenowy główny  1 kpl. serwer domenowy zapasowy |
| **Serwer główny** | 1. Obudowa: RACK 2U z możliwością instalacji do 8 dysków wraz z kompletem wysuwanych szyn 2. umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. 3. Procesor: Jeden procesor min. dziesięciordzeniowy z obsługą instrukcji 64 bitowych 4. umożliwiający osiągnięcie wyniku min. 10 000 punktów w teście PassMark CPU Benchmarks dostępnym na stronie <http://www.cpubenchmark.net/high_end_cpus.html> - wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim. 5. Procesor z obsługą wirtualizacji. 6. Pamięć: min. 128GB dedykowane do pracy serwerowej 7. Zainstalowane 1 dysk twardy SATA o pojemności min. 1TB. Dodatkowo 8 dysków SATA o pojemności minimum 4 TB każdy. 8. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s 9. Dodatkowa karta sieciowa: 10GbE, 1x SFP+ wraz z kablem DAC 5m SFP+ do SFP+ 10. Wsparcie KVM przez LAN 11. Panel przedni chroniący kluczem dostępu do dysków 12. Czujnik otwarcia obudowy 13. Komplet szyn montażowych w zestawie 14. 11. Gwarancja: minimum 2 lata gwarancji producenta. |
| **Serwer zapasowy** | 1. Obudowa: RACK 2U z możliwością instalacji do 8 dysków wraz z kompletem wysuwanych szyn 2. umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. 3. Procesor: Jeden procesor min. dziesięciordzeniowy z obsługą instrukcji 64 bitowych 4. umożliwiający osiągnięcie wyniku min. 10 000 punktów w teście PassMark CPU Benchmarks 5. dostępnym na stronie <http://www.cpubenchmark.net/high_end_cpus.html> - wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim. 6. Procesor z obsługą wirtualizacji. 7. Pamięć: min. 128GB dedykowane do pracy serwerowej 8. Zainstalowane 1 dysk twardy SATA o pojemności min. 1TB. Dodatkowo 8 dysków SATA o pojemności minimum 4 TB każdy. 9. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s 10. Dodatkowa karta sieciowa: 10GbE, 1x SFP+ wraz z kablem DAC 5m SFP+ do SFP+ 11. Wsparcie KVM przez LAN 12. Panel przedni chroniący kluczem dostępu do dysków 13. Czujnik otwarcia obudowy 14. Komplet szyn montażowych w zestawie 15. 10. Gwarancja: minimum 2 lata gwarancji producenta |
| **Oprogramowanie serwera zarządzania komputerami przy pomocy kontrolera**  **domeny** | 1. Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność: 2. interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO, 3. system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny, 4. serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS), 5. musi posiadać system antywirusowy, 6. możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3, 7. musi umożliwiać dostęp administratorów przez przeglądarkę WEB, 8. wbudowany firewall zarządzany przez przeglądarkę WEB, 9. przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB, 10. system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB, 11. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB, 12. W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność: 13. zarządzania do min. 130 użytkowników, grup, 14. zarządzanie do min. 130 komputerów, 15. zarządzanie do min. 130 urządzeń, 16. zarządzania polisami GPO, 17. obsługę profili użytkowników oraz profili mobilnych, 18. obsługę do min. 160 jednoczesnych podłączeń do serwera domeny, 19. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB, 20. możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB, 21. nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB, 22. wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB, 23. listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB, 24. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB, 25. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym, 26. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego, 27. administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB, 28. Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny. 29. Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny. 30. Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token, 31. Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny, 32. Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0, 33. Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u, 34. współpracy z klientami Windows 7,8,8.1,10 w wersji professional. 35. Licencja kontrolera domeny dla zamawianego serwera głównego i zapasowego musi umożliwiać: 36. łatwe przenoszenie i uruchomienie kontrolera domeny pomiędzy zamawianym serwerem głównym i zapasowym, 37. łatwe uruchomienie kontrolera domeny w trybie awaryjnym (w ograniczonej funkcjonalności) na dowolnym serwerze posiadanego przez zamawiającego na czas naprawy zamówionego serwera głównego lub zapasowego. 38. Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować: 39. obsługę minimum czterordzeniowego procesora, 40. obsługę minimum 32GB RAM-u, 41. obsługę vmware VMDK, 42. obsługę minimum 10 instancji środowisk wirtualnych, 43. zapis stanu maszyny wirtualnej tzw. snapshot, 44. kopii stanu maszyny wirtualnej, 45. emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS, 46. dynamicznej alokacji pamięci na kontener danych 47. współpracy z kontrolerami SATA, SCSI, 48. tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci, 49. zarządzanie poprzez przeglądarkę WEB, 50. archiwizacje uruchomionych maszyn wirtualnych. 51. Oprogramowanie musi również umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista,7,8,8.1,10 w wersji 32 i 64 bity w wersji professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 130 użytkowników i musi realizować: 52. automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego, 53. automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL, 54. automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego 55. automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.   Dostarczone oprogramowanie musi posiadać wsparcie techniczne i prawo do aktualizacji na okres min. 2 lat. |
| **Szkolenie i wdrożenie** | W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług:  1) wdrożenie serwerów:  Wykonawca stworzy plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie Głównego oraz Zapasowego serwera domenowego w szafie rack zamawiającego.  · montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów.  · Uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera.  · podłączenia Serwera do Przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera  · testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania  · instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie  2) szkolenie z dostarczonego rozwiązania:  \* szkolenie minimum 5 godzin na miejscu u Zamawiającego  \* zakres tematyczny:  omówienie fizycznych interface’ów sprzętu  - sposoby montażu w szafie RACK  - sposoby podłączenia kart rozszerzeń (np. dodatkowych kart)  - konfiguracja kontrolera pamięci masowej, tworzenie RAID  - ustawienia BIOS  - bezpieczeństwo  - zarządzanie niskopoziomowe  · przeprowadzenia szkolenia z zarządzania niskopoziomowego dostarczanych serwerów obejmującą:  o tworzenie grup RAID  o zdiagnozowanie ewentualnych problemów  o generowanie logów  Omówienie tworzenie nowych maszyn wirtualnych oraz ich parametryzację (zarządzanie wirtualnymi kartami sieciowymi, pamięcią ram)  o przedstawienie oraz charakterystyka oprogramowania do zarządzania środowiskiem wirtualizatorów  o konfiguracje wirtualnej infrastruktury sieciowej (wirtualnego przełącznika) |
| **Ilość** | 1. kpl. |

## Część II przedmiotu zamówienia

## Przełączniki sieciowe wraz ze szkoleniem

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Wymagania ogólne** | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. |
| **Wymagane parametry fizyczne** | Wymagane parametry fizyczne   1. możliwość montażu w szafie 19” 2. jeden wewnętrzny zasilacze 230V AC typu hot-swap. Z możliwością dołożenia dodatkowe zasilacza o tych samych parametrach. (nie dopuszcza się rozwiązań zewnętrznych zasilaczy)   port USB umożliwiający podłączenie zewnętrznej pamięci flash |
| **Wymagana konfiguracja portów** | Przełącznik musi posiadać minimum:   * 48 portów gigabitowych w standardzie 100/1000BaseT * Minimum 2 porty 1Gb SFP, pozwalające na instalację wkładek Gigabitowych (SFP) oraz możliwością podwyższenia prędkości portu do 10Gb za pomocą licencji. * Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Zamawiający wymaga, aby 1 port były obsadzony wkładką światłowodową typu SFP+ SR, oraz aby 1 port były obsadzony wkładką światłowodową typu SFP+ LR   Wszystkie powyższe porty muszą być dostępne od frontu urządzenia. |
| **Przełącznik** | Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:   1. Zarządzanie stosem poprzez jeden adres IP 2. Do min. 8 jednostek w stosie 3. Magistrala statkująca o wydajności 40 Gb/s 4. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie 5. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree 6. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.   Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów SFP+ w takim wypadku wymagane jest aby wraz z przełącznikiem dostarczony został kabel do stackowania 10GE SFP+ od długości minimum 1m. |
| **Matryca przełączająca** | Matryca przełączająca o wydajności min. 216 Gbps, wydajność przełączania przynajmniej 160 Mpps.  Obsługa min 16 000 adresów MAC  Wbudowana pamięć RAM min. 1 GB  Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB  Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)  Obsługa ramek jumbo o wielkości min. 9 216 bajtów  Obsługa protokołu GVRP lub równoważny  Wsparcie dla protokołów:   * IEEE 802.1w Rapid Spanning Tree * IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu.   Ethernet Ring Protection version 2  Obsługa min. 256 tras dla routingu IPv4  Obsługa min. 128 tras dla routingu IPv6  Obsługa protokołów routingu minimum:   * IPv4: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).   IPv6: minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).  Obsługa protokołów LLDP i LLDP-MED.  Przełącznik musi posiadać funkcjonalność DHCP Server  Obsługa ruchu multicast:  IGMP Snooping v1, v2 i v3  Obsługa mechanizmu DHCP snooping |
| **Mechanizmy związane z zapewnieniem bezpieczeństwa sieci** | Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:   1. min. 4 poziomy dostępu administracyjnego poprzez konsolę 2. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL 3. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www 4. zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 5. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP 6. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),   możliwość synchronizacji czasu zgodnie z NTP  Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:  klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP  Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3. |
| **Wymagane opcje zarządzania** | 1. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, 2. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), 3. urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,   dedykowany port konsoli zgodny ze standardem RS-232, |
| **Dodatkowe** | Wraz z urządzeniami muszą zostać dostarczone:   1. pełna dokumentacja w języku polskim lub angielskim, 2. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.   Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.  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 wymaga dostarczenia wraz z ofertą dokumentów potwierdzających ważność uprawnień gwarancyjnych na terenie Polski. |
| **Gwarancja** | Zamawiający wymaga, aby przełącznik posiadał 5-letni serwis gwarancyjny na sprzęt. Wymiana uszkodzonego elementu w trybie 8x5xNBD.  Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres eksploatacji urządzeń |
| **Wdrożenie** | W ramach dostawy Wykonawca zobowiązany jest do przeprowadzenia wdrożenia wraz ze szkoleniem w siedzibie Zamawiającego z dostarczonego sprzętu wraz z oprogramowaniem do zarządzania siecią przewodową.  Zakres minimalny wdrożenia:  - konfiguracja stosu z 4 przełączników (w ramach jednej szafy)  - konfiguracja do 20 VLAN'ów,  - wykonanie usługi routing między VLAN'ami na przełącznikach,  - wdrożenie NAC - 802.1x  Czas trwania wdrożenia oraz szkolenia nie może być krótszy niż:  - 5 dniowe wdrożenie sprzętu w siedzibie Zamawiającego  - 2 dniowe szkolenie dla 3 osób z konfiguracji/obsługi w/w rozwiązań w siedzibie Zamawiającego |
| **Oprogramowanie do zarządzania siecią przewodową** | W ramach dostawy Zamawiający wymaga dostarczenia oprogramowania do zarządzania siecią, spełniającą wymagania minimalne:  Architektura i zarządzanie  1. Dedykowane oprogramowanie służące do zarządzania i monitorowania pracy wszystkimi przełącznikami opisanymi w tym zamówieniu. Należy zapewnić licencję na obsługę min. 10 aktywnych urządzeń sieciowych (przełączniki)  2. System Zarządzania i Monitoringu musi być tego samego producenta co urządzania LAN  3. Oprogramowanie musi mieć możliwość instalacji w środowisku wirtualnym Vmware, Hyper-V i KVM  4. Obsługa musi być możliwa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW  5. Oprogramowanie musi pracować w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego miejsca w sieci (po uzyskaniu odpowiednich uprawnień),  6. Funkcja definiowania poziomu dostępu dla administratorów (wymagana jest możliwość profilowania kont administratorskich a użytkownikami Active Directory) z przypisanymi:  a. Rolami  b. Segmentami sieci, do których uzyskuje się dostęp  7. Oprogramowanie musi umożliwiać zbieranie statystyk w wykorzystaniem SNMP;  8. Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania.  9. Możliwość podglądu obecnej aktywnej konfiguracji z konfiguracją aktywną w zadanym historycznym momencie z podglądem elementów: dodanych, usuniętych, zmienionych względem danych konfiguracji.  10. Możliwość wysyłania alarmów mailem i SMS'em w przypadku wystąpienia zdarzeń określonych jako krytyczne  11. Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta  12. Lokalizowanie użytkowników po adresie nazwie sieciowej użytkownika, IP oraz MAC  13. Oprogramowanie musi posiadać narzędzia do automatycznego wykrywania urządzeń sieciowych instalowanych w sieci,  14. Oprogramowanie musi umożliwiać aktualizację oprogramowania w urządzeniach sieciowych,  15. Oprogramowanie musi posiadać narzędzia pozwalające na:  a. graficzną prezentację topologii sieci, w tym również graficzną, prezentację/budowę serwerowni lub dowolnego węzła sieciowego  b. konfigurację i monitoring sieci VLAN,  c. lokalizację oraz uzyskanie informacji o aktywności urządzeń w sieci,  16. Obrazowanie sieci w postaci mapki w tym lokalizacją urządzeń za pomocą Google Maps wraz z wyróżnianiem kolorami występujących alarmów na danych urządzeniach  17. Oprogramowanie musi umożliwiać zbieranie informacji o nieprawidłowych parametrach pracy zainstalowanego sprzętu wraz z możliwością generowania alertów o błędach czy przekroczeniu założonych parametrów (środowiskowych, wydajnościowych, dotyczących bezpieczeństwa),  18. Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA w szczególności funkcja monitorowania jakości oraz ilości połączeń Unified Communication and Collaboration.  19. Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach  20. Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępnie nie tylko monitorowanie, ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń, które powinno odbywać się za pomocą:  a. Autoprovisioningu urządzeń – czyli urządzenie podpięte do sieci bez konfiguracji powinno zgłosić się do oprogramowania do zarzadzania siecią o dedykowną dla urządzenia konfiguracje  b. Konfiguracja za pomocą Web GUI min. VLAN, IP Interfejsy, QoS, ACL  c. CLI Scripting – czyli możliwość przygotowania zbiorowej konfiguracji dla przełączników wraz ze zmiennymi w zależności modelu urządzenia  Moduł zabezpieczenie dostępu do sieci LAN  1. Oprogramowanie musi umożliwiać Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x w tym musi posiadać wewnętrzny serwer uwierzytelniający, pozwalający na integracje z usługami Active Directory  2. Licencje oprogramowania muszą umożliwiać integracja z Active Directory/LDAP w tym profilowanie użytkowników poprzez atrybuty AD/LDAP minimalnie:  a. Profilowanie użytkownika łączącego się do sieci bezprzewodowej z zależności od przypisania użytkownika do grupy AD/LDAP  b. Profilowanie użytkownika łączącego się do sieci bezprzewodowej z zależności od posiadanego systemu operacyjnego.  c. Poprzez profilowanie rozumiane jest:  i. przypisanie urządzeń użytkownika do zdefiniowanego VLAN  ii. nadanie urządzeniom polityk QoS  iii. nadanie urządzeniom dostępu lub uniemożliwienie dostępu do konkretnych segmentów sieci (ACL L2/L3/L4 oraz L7 – warstwa aplikacyjna)  Moduł dostęp gościnny  1. Samodzielna rejestracja klientów gościnnych w oparciu o:  a. Adres e-mail  b. Numer telefonu (wiadomość SMS)  2. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)  3. Logowanie w oparciu o portale społecznościowe min. Google, Facebook  4. Funkcja personalizacji strony gościnnej w tym obsługa portalu WiFi4EU  Gwarancja  Minimum 5 lat, umożliwiające min. kontakt z działem technicznym, rozwiązywanie problemów, możliwość aktualizacji oprogramowania do najnowszej wersji. |
| **Ilość** | 4 kpl. |

## Część III przedmiotu zamówienia

## Oprogramowanie do szyfrowania poczty wraz ze szkoleniem

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie do szyfrowania poczty wraz ze szkoleniem |
| **Wymagania techniczne** | W ramach dostawy Wykonawca zobowiązany jest do dostarczenia oprogramowania do szyfrowania wiadomości e-mail technologią “end to end” dla 100 użytkowników.  Dostarczone oprogramowanie musi zapewnić funkcjonalność minimalną:  - szyfrowanie algorytmem AES256 treści wiadomości,  - szyfrowanie algorytmem AES256 załączników,  - szyfrowanie algorytmem AES256 plików,  - szyfrowanie algorytmem AES256 katalogów,  - do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest  dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu  internetowego.  - do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest  połączenie Internetowe.  - do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania  deszyfrującego.  - do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego.  - odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na  popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista,  Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Ubuntu Desktop 20.04.3, Ubuntu  Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0  - szyfrowana zawartość wiadomości może zawierać nie tylko tekst,ale również elementy graficzne  takie jak: HTML, obrazki  - generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla  szyfrowania,  - opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej  oryginalność,  - zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,  - posiadania wewnętrznej bazy haseł, która umożliwia:   1. export haseł do pliku, 2. import haseł z pliku 3. generowania ponownie haseł w bazie   - posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,  - posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym  hasłem szyfrującym,  - posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych,  plików i katalogów,  - pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią  lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system  pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows.  - integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,  - zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,  - wykrywania fałszywych emaili - Antiphishing,  - wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,  - wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,  - wykrywanie niebezpiecznych dokumentów MS Office,  - wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,  - definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,  - współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 4 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlanie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 4 razy w ciągu dnia,  - alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc,  - współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64  Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11. |
| **Wymagania dodatkowe** | Oprogramowanie musi zostać dostarczone wraz z licencją wieczystą na użytkowanie oprogramowania z wsparciem technicznym i prawem do aktualizacji oprogramowania, bazami reguł, sygnatur i zagrożeń phishing przez minimum 48 miesięcy.  Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych licencji na oprogramowanie dodatkowe.  Oprogramowanie musi poprawnie działać z wykorzystywanym oprogramowaniem antywirusowym posiadanym przez Zamawiającego tj. ESET ENDPOINT ANTYVIRUS ważnego do dnia 25.04.2023  Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.  Uwierzytelnienie użytkowników do systemu operacyjnego i kontrolera domeny musi odbywać się przy pomocy dedykowanego urządzenia sprzętowego. W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostarczenia 100 urządzeń autoryzacyjnych typu TOKEN, o wymaganiach minimalnych:  - Pamięć urządzenia sprzętowego musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domenowego.  - Możliwość autoryzacji do systemu operacyjnego i kontrolera domeny musi być realizowana dedykowanym min. 6 znakowym PIN-em.  - Użytkownik zanim dokona logowania do systemu operacyjnego przy pomocy urządzenia sprzętowego musi mieć możliwość wyświetlenia zdefiniowanej przez administratora wewnętrzną PBI.  - Administrator Bezpieczeństwa Informacji musi mieć możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego i kontrolera domeny.  - Ważność certyfikatu bezpieczeństwa wystawianego przez producenta dla urządzeń autoryzujących typu TOKEN: minimum 48 miesięcy |
| **Wdrożenie i szkolenie** | W ramach realizacji dostawy przedmiotu zamówienia, Wykonawca zobowiązany do przeprowadzenia wdrożenia rozwiązania na miejscu u Klienta, wraz z przeprowadzeniem szkolenie z zakresu użytkowania oprogramowania dla min. 2 administratorów, w zakresie min. 4 godzin. |
| **Ilość** | 1 kpl. |

## Część IV przedmiotu zamówienia

## UPS

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zasilanie awaryjne UPS |
| **Wymagania minimalne** | W ramach realizacji dostawy Wykonawca zobowiązany jest do:  dostarczenia urządzeń UPS podtrzymujących zasilanie spełniającymi wymagania minimalne określone poniżej  do przeprowadzenia demontażu posiadanych przez Zamawiającego urządzeń UPS  do montażu dostarczonych urządzeń UPS wraz z usługą przełożenia posiadanych przez Zamawiającego akumulatorów bateryjnych  Wymagania ogólne: minimum 15kW  Ilość: min. 4 sztuki  Moc znamionowa wyjściowa (wsp. mocy 1,0): minimum 8, 10, 15, 20  Ilość baterii wewnętrznych: minimum 0 do 2 x 32 bloki  Możliwość rozbudowy: Tak, do 20 kW  Topologia UPS: Podwójna konwersja  Sprawność w trybie podwójnej konwersji: min. >96%  Sprawność w trybie podwyższonej sprawności energetycznej (ESS): min. Do 99%  Stopień ochrony UPS: IP 20  Urządzenia musi być kompatybilne z posiadanymi przez Zamawiającym akumulatorami (256 szt.) MWH 9-12L Bateria 12V; 9Ah/270W faston (250), |
| **Wejście** | Napięcie znamionowe (konfigurowalne): 220/380 V; 230/400 V; 240/415 V  Znamionowa częstotliwość wejściowa: 50 lub 60 Hz, konfigurowalna przez użytkownika  Tolerancja częstotliwości: min. 40 do 72 Hz  Przewody wejściowe: 3F + Neutralny  Możliwość ‘miękkiego startu’  Wewnętrzne zabezpieczenie wsteczne: Tak, dla obwodu prostownika i bypassu |
| **Wyjście** | Przewody wyjściowe: min. 3F + Neutralny  Napięcie znamionowe: min. 220/380 V; 230/400 V; 240/415 V, (konfigurowalne) |
| **Komunikacja** | MiniSlot: 2 sloty komunikacyjne  Interfejs sieciowy / SNMP: Tak, standardowo  Porty komunikacyjne min.:  - porty mini-slot na opcjonalne karty komunikacyjne,  - min. 1 x USB dla urządzeń,  - min. 1 x USB hosta,  - min. 1 port serwisowy RS-232,  - min. 1 x wyjście przekaźnikowe,  - min. 5 x wejść alarmów budynkowych oraz dedykowany EPO,  - min. 1 x karta internetowa i SNMP |
| **Bezpieczeństwo** | Bezpieczeństwo (certyfikacja CB) min. IEC 62040-1 lub równoważna  EMC: min. IEC 62040-2 lub równoważna  Parametry: min. IEC 62040-3 lub równoważna |
| **Wymagania dodatkowe** | Zamawiający wymaga, aby do każdego zasilacza zostały dołączone po minimum 2 gałęzie bateryjne (battery kit) |
| **Gwarancja** | Minimum 24 miesięczna gwarancja na wady fizyczne i prawne towarów od daty uruchomienia potwierdzonej odpowiednim protokołem, nie dłużej niż 27 miesięcy od daty dostawy. |
| **Usługi** | W trakcie instalacji ma zostać zastosowany bypass serwisowy wraz z niezbędnym okablowaniem do podłączenia.  Zamawiający wymaga, aby uruchomienie zasilacza zostało wykonane przez autoryzowany serwis producenta lub osoby upoważnione i aby zostało przeprowadzone szkolenie z podstawowej obsługi na miejscu u Zamawiającego w zakresie minimum 4 h. |
| **Ilość** | 1. kpl. |

## Część V przedmiotu zamówienia

## Urządzenie do backupu - typ I

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie do backupu |
| **Procesor** | Min. AMD Ryzen V1500B 4-core 2.2 GHz |
| **Obudowa** | Rack 2U o wymiarach 88 × 482 x 306,6 mm |
| **Montaż RACK** | Tak; do szafy RACK 19’ |
| **Pamięć RAM** | Minimum 16GB pamięci DDR4 (1 x 16GB) |
| **Ilość obsługiwanych dysków** | 8 dysków o maksymalnej pojemności 16TB każdy z możliwością podłączenia zewnętrznej półki, która rozszerza pojemność serwera o kolejne 4 dyski |
| **Zamontowane dyski twarde** | Zamontowane 8 dysków twardych, każdy o pojemności 8TB znajdujące się na liście kompatybilności producenta oferowanego urządzenia NAS, spełniające wymagania: SATA 6 Gb/s, MTBF min 1000000h, 128MB pamięci podręcznej, 5400 obr./min., gwarancja producenta 3 lata, |
| **Interfejsy sieciowe** | 4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation |
| **Porty** | 2 x USB 3.2, 1 x eSATA, 1x PCIe 3 x 4-liniowe gniazdo x8, port konsoli x1 |
| **Wskaźniki LED** | Power on, Status, HDD1 -8 |
| **Obsługa RAID** | Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR, RAID 1,5,6,10 |
| **Funkcje RAID** | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| **System Operacyjny** | Windows 7 i 10, Mac OS X® 10.11 i nowszy |
| **Licencja na Kamery IP** | W zestawie dwie licencje na jedną kamerę z możliwością rozszerzenia do 40. |
| **Protokoły** | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| **Usługi** | Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Hyper Backup, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Cloud Station, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, Snapshot Replication, MailPlus Serwer, Virtual Machine Manager, Active Backup Suite, Chat, Office, Klaster SHA |
| **Obsługa migawek** | • Maksymalna liczba migawek folderów współdzielonych: 1 024  • Maksymalna liczba migawek systemu: 65 536 |
| **Zarządzanie dyskami** | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, |
| **Język GUI** | Polski, Angielski |
| **Gwarancja i serwis** | 3 lata gwarancji producenta |
| **Waga** | 6,9 KG |
| **Pobór mocy** | Max. 50W / Hibernacja dysków max. 23W |
| **Certyfikaty** | EAC, VCCI, CCC, RCM, KC, FCC, CE, BSMI |
| **System plików** | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) |
| **Liczba wolumenów** | Do 64 |
| **Liczba iSCSI Targetów** | Do 128 |
| **Liczba iSCSI LUN** | Do 256 |
| **Liczba kont użytkowników** | 2048 |
| **Liczba grup** | 256 |
| **Liczba udziałów** | 512 |
| **Ilość jednoczesnych połączeń** | 1000 dla CIFS/AFP/NFS/FTP/WebDAV; 2,000 po rozszerzeniu RAM |
| **Zasilanie** | Zasilacz 250W |
| **Chłodzenie** | FAN x 2 80 x 80 mm |
| **Ilość** | 1 szt. |

## Urządzenie do backupu - typ II

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie do backupu |
| **Wymagania minimalne** | W ramach dostawy Zamawiający wymaga dostarczenia kompleksowego, zintegrowanego rozwiązania do backupu wraz z usługą wdrożenia zdalnego oraz pomocą techniczną wykonawcy na okres 1 roku.  System powinien umożliwić archiwizację 10 stacji roboczych. |
| **Wymagania sprzętowe** | * Obudowa: tower * Procesor: minimum czterordzeniowy * Pamięć: min. 4 GB * Ilość obsługiwanych dysków: 4 dysków o maksymalnej pojemności 18TB każdy, po podłączeniu modułu rozszerzającego 9 dysków; 2 dyski M.2 2280 NVMe SSD * Zamontowane wewnętrzne dyski twarde kompatybilne z urządzeniem: dwa dyski twarde 4TB znajdujące się na liście kompatybilności producenta oferowanego urządzenia NAS spełniające wymagania: SATA 6 Gb/s, 3,5”, 64MB pamięci podręcznej, 5900 obr./min, MTBF min 1000000 h, gwarancja producenta 3 lata * Dyski z możliwością wymiany podczas pracy (hot-swap) * Obsługiwane typy macierzy RAID: Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6 (z dodatkową jednostką rozszerzającą), 10 (z dodatkową jednostką rozszerzającą), * Funkcje RAID: Możliwość zwiększania pojemności i migracja między poziomami RAID online * Porty: 2 x USB3.2 gen 1, 1 x eSATA * Wskaźniki LED: Status, HDD1-4, Power on * Port LAN RJ-45: 2 x Gigabit (10/100/1000) Wsparcie dla Link Agregation * System plików: Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) * Protokoły: SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) * Usługi: Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Hyper Backup, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Cloud Station, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, Snapshot Replication, MailPlus Serwer, Virtual Machine Manager, Active Backup Suite, Chat, Office, Możliwość pracy oferowanego serwera w klastrze HA * Zasilacz min. 100W |
| **Wymagania funkcjonalne** | * Możliwość backupu stacji roboczych, serwerów, maszyn wirtualnych. * Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, * z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich * Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019 Linux, BSD, Mac OS X * Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, Linux, BSD, Mac OS X, QNAP, Synology * Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) * Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) * Automatyczny backup przy wyłączaniu komputera (tylko Windows) * Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ? * Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows) * Backup baz danych i plików poczty w trybie online i offline * Kopie rotacyjne (wersjonowanie) * Zapis archiwów w otwartym formacie (ZIP 64-bit) * Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi * Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) * Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej * Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych * Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO * Możliwość określenia liczby archiwów przechowywanych w miejscu replikacji (mniej lub więcej niż miejscu źródłowym) * Kompresja po stronie stacji roboczej * Replikacja archiwów (automatyczna lub według harmonogramu) na dodatkowy dysk twardy, NAS, serwer FTP, * Centralne sterowanie całym Systemem z jednego miejsca * Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników * Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN * Wysyłanie Alertów administracyjnych na e-mail * Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych * Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki * Automatyczna aktualizacja oprogramowania na komputerach zdalnych * Bezterminowa licencja - licencja nie może być ograniczona czasowo * Interfejs, instrukcja i pomoc techniczna w języku polskim * Rozmiar instalacji klienta < 1MB |
| **Wdrożenie** | W ramach dostawy Zamawiający wymaga, aby została przeprowadzona usługa wdrożenia, w formie zdalnej, a w jej zakresie powinny zawierać się przynajmniej:  • Wysyłka przygotowanej do wdrożenia macierzy NAS (przeprowadzona integracja  z oprogramowaniem do backupu),  • Konfiguracja serwera backupu,  • Przygotowanie paczki instalacyjnej aplikacji klienta backupu,  • Omówienie i konfiguracja zadań backupu dla najważniejszych stacji klienckich  • Instruktażowe szkolenie administratora z wdrożonego systemu obejmujące przynajmniej omówienie procesu odzyskiwania danych oraz omówienie funkcji konsoli administracyjnej. |
| **Gwarancja** | Minimum 3 lata |
| **Ilość** | 1 szt. |

## 

## Część VI przedmiotu zamówienia

## Stacje robocze

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| **Procesor** | Procesor osiągający w teście PassMark CPU Mark wynik min. 17 000 punków według wyników ze strony <https://www.cpubenchmark.net> wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim. |
| **Pamięć RAM** | Zainstalowane min. 8 GB RAM min. 3200MHz  Zapewnienie maksymalnej obsługiwanej pojemności minimum 64 GB  Trzy sloty pamięci wolne. |
| **Pamięć masowa** | Dysk o pojemności min 500GB z interfejsem M.2 NVMe gen4 |
| **Wydajność grafiki** | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki.  Pełna obsługa funkcji i standardów DX12, OpenGL 4.5, OpenCL 3.0. 2.5.3. Możliwość zainstalowania dodatkowej, dedykowanej karty graficznej z pamięcią własną min. 4 GB.  Grafika zintegrowana w procesorze musi umożliwiać jednoczesną obsługę co najmniej dwóch monitorów. |
| **Płyta główna** | Rozmiar ATX  Rodzaje wejść / wyjść - panel przedni:  - minimum 2 x USB, w tym min. 1 porty USB 3.2 Gen 1,  - wejście mikrofonowe i wyjście słuchawkowe 1 szt.  Rodzaje wejść / wyjść - panel tylny:  - USB 2.0 - 2 szt.  - USB 3.1 Gen. 1 (USB 3.0) - 4 szt.  - RJ-45 (LAN) - 1 szt.  - HDMI - 1 szt.  - D-sub  - 5.1-kanałowy dźwięk  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.  Złącza wewnętrzne:  - 1 x złącze PCIe 3.0 x16  - 1 x złącze PCIe 3.0 x1  - 4 x port SATA 6 Gb/s  - 2 x M.2 dla dysku SSD |
| **Karta sieciowa** | Minimum 1 karta sieciowa 1 Gigabit zintegrowana z płytą główną. |
| **Zasilacz** | Zasilacz o mocy min 500 W. Certyfikat sprawności minimum: 80 Plus Gold |
| **Dodatkowe** | Zamawiający wymaga, aby dostarczone stacje robocze posiadały dodatkowo:  Mysz: przewodowa USB, optyczna, z dwoma przyciskami i scrollem, min. 800dpi, kolor czarny  Klawiatura: przewodowa USB (układ polski programisty), kolor czarny  Listwa zasilająca przepięciowa: ilość gniazd AC: minimum 5 sztuk, włącznik, sygnalizacja działania poprzez podświetlany przycisk zasilania, bezpiecznik, kolor czarny  Kamera: łączność interfejs min. USB 2.0 Plug & Play, mikrofon wbudowany mono, rozdzielczość FullHD (1920 x 1080) kąt widzenia min. 70°, sposób montażu - uniwersalny klips  Głośniki: minimalny typ zestawu 2.0 - 2 głośniki, moc wyjściowa głośników min. 2x 2,2W RMS, typ podłączenia jack 3,5 mm, zasilanie za pomocą kabla USB 2.0, regulacja głośności na głośniku |
| **Wyposażenie multimedialne** | Karta dźwiękowa min. czterokanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera**.** Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out. |
| **Obudowa** | Typu MidiTower z obsługą kart PCI Express wyłącznie o pełnym profilu.  Obudowa fabrycznie przystosowana do pracy w orientacji pionowej.  Obudowa wyposażona w dystanse zapobiegające poślizgom obudowy i zarysowaniu lakieru.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie  Zamawiający nie dopuszcza, aby dostarczony sprzęt komputerowy posiadał plomb zabezpieczających przed samodzielnym otwarciem obudowy komputera  Kolor czarny |
| **Bezpieczeństwo** | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.  Procedura POST traktowana jest jako oddzielna funkcjonalność. |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **Zgodność z systemami operacyjnymi i standardami** | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi. |
| **System operacyjny** | Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Licencja bezterminowa zapewniająca prawo do wykorzystywania przez jednostki samorządu terytorialnego. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych:   lupa powiększająca zawartość ekranu,   * narrator odczytujący zawartość ekranu, * regulacja jasności i kontrastu ekranu, * możliwość odwrócenia kolorów np. biały tekst na czarnym tle, * poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, * funkcja sterowania myszą z klawiatury numerycznej, * funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, * korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, * funkcja napisów w treściach wideo, * możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków;  1. Możliwość zarządzania stacją roboczą poprzez polityki. 2. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 3. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 4. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 5. 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. 6. Graficzne środowisko instalacji i konfiguracji. 7. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 8. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 9. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 10. Możliwość przywracania plików systemowych.   Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). |
| **Certyfikaty i standardy** | Certyfikat ISO9001 lub równoważny dla producenta sprzętu  Deklaracja zgodności CE lub inny równoważny  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważną |
| **Monitor** | Typ ekranu: ekran ciekłokrystaliczny z aktywną matrycą IPS min. 23,8” .  Jasność: 250 cd/m2.  Kontrast: 1000:1.  Kąty widzenia (pion/poziom): 178/178 stopni.  Czas reakcji matrycy (maksymalnie): 5ms.  Rozdzielczość minimalna: 1920 x 1080.  Powłoka powierzchni ekranu: matowa.  Podświetlenie: system podświetlenia LED.  Złącza bez konieczności stosowania przejściówek minimum:  1x HDMI  1x D-sub  1x DVI  W zestawie kabel zasilający, kabel HDMI wersja min. 1.4.  Kolor czarny |
| **Warunki gwarancji** | Wymagane dołączenie do oferty dokumentu potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Minimalny czas trwania wsparcia technicznego producenta wynosi 36 miesięcy.  Sposób realizacji usług wsparcia technicznego:   * Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17.   Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Zamawiający wymaga dołączenia dokumentów potwierdzających, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| **Dodatkowe oprogramowanie** | Wymagane jest dostarczenie sprzętu wraz z zainstalowanym oprogramowaniem biurowym, który musi mieć zaimplementowane co najmniej następujące funkcjonalności tj. edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.  Wymagania odnośnie interfejsu użytkownika:  a) pełna polska wersja językowa interfejsu użytkownika,  b) możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO) w domenie,  c) całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie,  d) wsparcie dla formatu XML,  e) możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów,  f) możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony,  g) możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych, w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu,  h) prawidłowe odczytywanie i zapisywanie danych w dokumentach min. w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w tym plikach wytworzonych w MS Office 2007, MS Office 2010 i MS Office 2013, Office 2016, Office 2019  i) zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).  Musi być kompatybilny z posiadanym przez Zamawiającego oprogramowaniem Microsoft Office i pozwalać min. na:  a) otwieranie dokumentów utworzonych przy pomocy programów MS Word (od wersji 2007 do 2019), MS Excel (od wersji 2007 do 2019), MS Power Point (od wersji 2007 do 2019),  b) w otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (min.: korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze.) czy też konieczności dodatkowej edycji ze strony użytkownika.  Edytor tekstów musi umożliwiać min.:  a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,  b) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),  c) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,  d) automatyczne tworzenie spisów treści,  e) sprawdzanie pisowni w języku polskim,  f) śledzenie zmian wprowadzonych przez użytkowników,  g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,  h) określenie układu strony (pionowa/pozioma),  i) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego,  j) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Arkusz kalkulacyjny musi umożliwiać min.:  a) tworzenie raportów tabelarycznych,  b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,  c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,  d) tworzenie raportów z zewnętrznych źródeł danych (min. inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),  e) tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,  f) wykonywanie analiz danych przy użyciu formatowania warunkowego,  g) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,  h) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,  i) formatowanie czasu, daty i wartości finansowych z polskim formatem,  j) zapis wielu arkuszy kalkulacyjnych w jednym pliku,  k) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 do 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,  l) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać min. przygotowywanie prezentacji multimedialnych oraz:  a) drukowanie w formacie umożliwiającym robienie notatek,  b) zapisanie w postaci tylko do odczytu,  c) nagrywanie narracji dołączanej do prezentacji,  d) opatrywanie slajdów notatkami dla prezentera,  e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,  f) tworzenie animacji obiektów i całych slajdów.  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać min.:  a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,  b) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,  c) automatyczne grupowanie poczty o tym samym tytule,  d) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,  e) oznaczenie poczty elektronicznej z określeniem terminu przypomnienia,  f) zarządzanie kalendarzem,  g) zapraszanie uczestników na spotkanie, co po ich akceptacji musi spowodować automatyczne wprowadzenie spotkania w ich kalendarzach,  h) zarządzanie listą zadań,  i) zlecanie zadań innym użytkownikom,  j) zarządzanie listą kontaktów,  k) udostępnianie listy kontaktów innym użytkownikom,  l) przeglądanie listy kontaktów innych użytkowników,  m) możliwość przesyłania kontaktów innym użytkowników. |
| **Ilość** | 1. kpl. |

## Część VII przedmiotu zamówienia

## Urządzenie klasy UTM

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami oraz wdrożeniem i szkoleniem |
| **Wymagania techniczne** | * + - 1. Zapora sieciowa typu Next Generation Firewall (NGFW),       2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.       3. Minimalna ilość interfejsów:   a) 6 interfejsów 10 GbE SFP+,   * 1. 4 interfejsy 5 GbE SFP+,   2. 24 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.   3. 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,   4. 1 interfejs konsoli do zarządzania zaporą,   5. 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą,  1. Zapora powinna posiadać dysk M.2 o pojemności przynajmniej 128 GB z możliwością wymiany na większy. 2. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa 3. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji, 4. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q, 5. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej, 6. Minimalna ilość jednocześnie obsługiwanych połączeń: 2 000 000, 7. Możliwość obsłużenia przynajmniej 22 500 nowych połączeń w ciągu 1 sekundy. 8. Przepustowość urządzenia pracującego w trybie stateful firewall: 5,5 Gbps – dla ramki 1518B zgodnie z RFC 2544, 9. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 3.8 Gbps, 10. Przepustowość urządzenia pracującego jako koncentrator VPN: 2,2 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544, 11. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń, jeśli chodzi o wielkość skanowanych plików) – 3,5 Gbps, 12. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3 000, 13. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 500 14. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000. 15. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne. 16. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 850 Mbps oraz obsłużyć 150 000 połączeń. 17. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, 18. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site), 19. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa), 20. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, 21. Wsparcie dla Dynamicznego DNS tzw. DDNS, 22. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne. 23. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony, na które użytkownik wchodzi bezpośrednio). 24. Administrator powinien mieć możliwość tworzenia różnych akcji, dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:     1. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),     2. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,     3. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. 25. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps, 26. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL. 27. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci. 28. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. 29. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN), 30. Kontrola dostępności zestawionych tuneli VPN, 31. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. 32. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty. 33. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić) 34. Funkcja NAT oparta o reguły bezpieczeństwa. 35. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe), 36. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych. 37. Zintegrowany system skanowania antyspyware, 38. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www. 39. System IPS musi używać algorytmu szeregowego przetwarzania. 40. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex). 41. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,     1. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.     2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,     3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur. 42. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików. 43. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa, 44. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi, 45. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p, 46. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, 47. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji. 48. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. 49. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej. |
| **Gwarancja** | Min. 24 miesiące wraz ze wsparciem technicznym w trybie 24x7. |
| **Wymagania licencyjne** | Wraz z urządzeniem Zamawiający wymaga dostarczenia subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat.  Dodatkowe Zamawiający wymaga, aby posiadane aktywne subskrypcje na obecnie posiadanym urządzeniu SONICWALL ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 2600 ważne do dnia 16.04.2023 zostały przeniesione i dodane do subskrypcji oferowanego urządzenia. |
| **Wymagania dodatkowe** | W ramach dostawy Wykonawca zobowiązany jest do przeprowadzenia:  1) Wdrożenie  -Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, konfiguracja routingu, DNS, NTP),  -Konfiguracja profilów administracyjnych,  Podpięcie weryfikacja statusu licencji,  -Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy),  -Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa,  -Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa,  -Konfiguracja lokalnej bazy użytkowników oraz zdefiniowanie grup, oraz podłączenie do usługi LDAP/AD  Konfiguracja VPN wg potrzeby  -Konfiguracja IPSec VPN site-to-site,  --Konfiguracja IPSec VPN client-to-site,  -Konfiguracja SSL VPN client-to-site,  -Konfiguracja profilów kontroli Antywirusowej i podpięcie do polityk FW,  -Konfiguracja profilów ochrony przed atakami IPS i podpięcie do polityk FW,  -Konfiguracja profilów kontroli aplikacji i podpięcie do polityk FW,  -Konfiguracja profilów kontroli WWW i podpięcie do polityk FW,  -Konfiguracja profilów antyspamowych i podpięcie do polityk FW,  -Test zastosowanych funkcji ochronnych,  -Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji.  2) Instruktaż zdalny  Wymagane jest, aby wdrożenie oraz instruktaż został wykonany przez inżynierów certyfikowanych przez producenta dostarczonego rozwiązania klasy UTM (do oferty dołączyć certyfikaty inżynierów) w minimalnym zakresie:  -Przeszkolenie z zakresu zarządzania wszystkimi elementami podlegającymi konfiguracji w punkcie “Wdrożenie”  -Szkolenie musi trwać minimum 3h  -Szkolenie z odtwarzania konfiguracji po awarii urządzenia backup lokalny/backup z chmury producenta.  -Szkolenie dotyczące generowania logów  -Szkolenie dotyczące konfiguracji tuneli VPN w tym SSL VPN/IPSEC  -Przeszkolenie z zakresu prostych narzędzi do rozwiązywania problemów. |
| **Ilość** | 1 szt. |

## 

## Część VIII przedmiotu zamówienia

## Audyt bezpieczeństwa-

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla usługi** |
| **Typ** | Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina.  Diagnoza cyberbezpieczeństwa powinna zostać przeprowadzona w terminie do 60 dni od podpisania umowy.  Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza diagnozy i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Instytut/SkrytkaESP. |
| **Plan audytu** | Audyt musi składać się z minimum:  1. Audyt dokumentacji i procesów:  - ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)  - ocena wybranych aspektów bezpieczeństwa systemów informatycznych  - ocena dojrzałości wybranych procesów bezpieczeństwa  - opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny  2. Testy penetracyjne infrastruktury sieciowej  - Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci  - skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci)  - skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy  - sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy  - sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł  - weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych  - weryfikacja zabezpieczeń urządzeń sieciowych - testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej  - wykonanie raportu zawierającego minimum:   * opis wszystkich elementów, które zostały poddane audytowi * podział podatności ze względu na ryzyko: wysoki, średni, niski * wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności * wylistowanie wszystkich podatności ze względu na ryzyko: wysoki, średni, niski * określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności   - Wsparcie poaudytowe – Wykonawca ma obowiązek na udzielenie informacji na temat audytowanych elementów wynikających z raportu w terminie maksymalnie 7 dni od wykonania raportu. |
| **Wymagania dla audytora** | Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu:  1. Certified Internal Auditor (CIA);  2. Certified Information System Auditor (CISA);  3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001  wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r.  o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie  certyfikacji osób;  4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę  oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;  5. Certified Information Security Manager (CISM);  6. Certified in Risk and Information Systems Control (CRISC);  7. Certified in the Governance of Enterprise IT (CGEIT);  8. Certified Information Systems Security Professional (CISSP);  9. Systems Security Certified Practitioner (SSCP);  10. Certified Reliability Professional;  11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert |

## 

## Część IX przedmiotu zamówienia

## Szkolenia dla pracowników z zakresu cyberbezpieczeństwa

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenie zdalne dla pracowników Urzędu z zakresu cyberbezpieczeństwa |
| **Program szkolenia** | 1. Czym jest cyberbezpieczeństwo. 2. Podstawowe przedstawienie zagadnienia cyberbezpieczenstwa 3. Przedstawienie zagrożeń, które czyhają na nas w sieci (rodzaje zagrożeń i ich konsekwencje) 4. Opis i wymagania normy ISO/IEC 27001 5. Dlaczego wiedza o cyberbezpieczeństwie jest konieczna? 6. Sposoby ochrony kont i danych przed potencjalnym zagrożeniem. 7. Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności a co za tym idzie programy pomagające w tym (np. keypas) 8. Logowanie w sieci. 9. Opis Certyfikatów stron internetowych. 10. Darmowe WiFi i automatyczne podłączanie się. 11. Praca zdalna - czym jest VPN i jak z niego korzystać. 12. Wprowadzenie do sieci komputerowych - niebezpieczeństwo sieci otwartych bezprzewodowych. 13. Niezabezpieczone protokoły sieciowe - HTTP FTP 14. Zaszyfrowana komunikacja w Internecie (Signal i WhatsApp) 15. Ochrona plików i dysków czyli podstawy szyfrowania. 16. Przedstawienie przykładów i nauka rozpoznawania niepożądanych maili i ich zawartości. 17. Odpowiednia weryfikacja odbiorcy i nadawcy. 18. Weryfikacją wiadomości e-mail 19. Weryfikacja i skan plików znajdujących się w załączniku. 20. Przykłady ataków oraz sposoby na ochronę przed nimi pod kątem zwykłego użytkownika 21. Phishing i td - Sposoby na zabezpieczenie się przed włamaniami i oszustwem w sieci 22. Programy antywirusowe i ich rola (omówienie popularnych programów i opis ich działania) 23. Tworzenie kopii zapasowych i ich odzyskiwanie po awarii. 24. Sposoby tworzenia backup’ów. 25. Podpis elektroniczny dokumentów w prosty i bezpieczny sposób. |
| **Wymagania dodatkowe** | W ramach realizacji szkolenia wymagane jest, aby:  - Szczegółowy harmonogram szkolenia został uzgodniony z Zamawiającym terminie minimum 14 dni przed terminem rozpoczęcia szkolenia  - Szkolenia zostaną przeprowadzone w maksymalnie 2 turach po 4 godziny  - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych,  - Uczestnik po zakończeniu szkolenia musi otrzymać zaświadczenie ukończenia szkolenia - Uczestnik musi mieć możliwość bezpłatnego 14-sto dniowego kontaktu z trenerem po szkoleniu. |
| **Ilość** | Szkolenie dla 80 pracowników |

# 

# **Wymagania dodatkowe**

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostawy przedmiotu zamówienia wraz z jego rozpakowaniem, sprawdzeniem poprawności działania i ustawieniem w wyznaczonym przez Zamawiającego pomieszczeniu na terenie Urzędu.

Wykonawca zobowiązany do utylizacji na własny koszt wszelkich niepotrzebnych materiałów zabezpieczających urządzenia podczas transportu, w tym kartony, folie, taśmy klejące etc.

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.