Załącznik nr 5 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiot zamówienia obejmuje:

1. 2 komputery przenośne
2. 8 komputerów stacjonarnych z monitorami
3. 4 zasilacze awaryjne UPS do komputerów stacjonarnych
4. 1 zasilacz awaryjny do serwerów
5. 1 przełącznik zarządzalny
6. 2 urządzenia do ochrony połączenia internetowego z licencją na 12 miesięcy na potrzeby szkół
7. 1 dysk sieciowy NAS do archiwizacji danych
8. 1 skaner dokumentów do elektronicznego obiegu dokumentów
9. 2 komputery przenośne

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Wymagane minimalne parametry techniczne** |
|  | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i5-1135G4 na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |
|  | Pamięć operacyjna RAM | Min. 8 GB 3200 MHz non-ECC  Możliwość rozbudowy pamięci do min. 40GB |
|  | Parametry pamięci masowej | M.2 256 GB SSD PCIe NVMe  Dostępny drugi slot M.2 na dysk SSD.  Możliwość rozbudowy do konfiguracji dwudyskowej. |
|  | Karta graficzna | Zintegrowana z procesorem |
|  | Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute). |
|  | Obudowa | Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H  *Jako potwierdzenie parametrów wytrzymałościowych należy dostarczyć kartę katalogową producenta komputera lub jego oświadczenie dotyczące oferowanego modelu.* |
|  | Płyta główna | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. |
|  | Zgodność z systemami operacyjnymi | Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym.  *Jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy* |
|  | Bezpieczeństwo | TPM 2.0  Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington |
|  | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:  - wersji BIOS  - nr seryjnym komputera  - Ilości zainstalowanej pamięci RAM  - typie procesora i jego prędkości  - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS    Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:  -Możliwość ustawienia hasła Administratora  -Możliwość ustawienia hasła Użytkownika  -Możliwość ustawienia hasła dysku twardego  -Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS  -Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej.  -Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth |
|  | Ekran | Matowy, matryca TFT 15” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 300nits, kontrast 800:1 w technologii IPS/PLS/WVA  Kąt otwarcia pokrywy ekranu min.180 stopni. |
|  | Interfejsy / Komunikacja | 4xUSB 3.2 z czego minimum 2 złącza Typu-C umożliwiające podłączenie stacji dokującej lub zasilania notebooka i dodatkowego ekranu (niezależnie od wybranego portu USB-C). Złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 1.4b, RJ-45. Komputer musi obsługiwać komunikację Thunderbolt 4 za pomocą min. 1 złącza USB-C. Czytnik kart pamięci. |
|  | Karta sieciowa WLAN | Wbudowana karta sieciowa, pracująca w standardzie AX 2x2  Bluetooth 5.1 |
|  | Klawiatura | Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.  *Zamawiający wymaga dostarczenia karty katalogowej producenta potwierdzającej odporność klawiatury na zalanie cieczą.* |
|  | Czytnik linii papilarnych | Wbudowany czytnik linii papilarnych w przycisku zasilania |
|  | Akumulator | Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – *należy załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym.* Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 60 minut od 0% do 80%. |
|  | Zasilacz | Zasilacz zewnętrzny 65W |
|  | Certyfikaty, oświadczenia i standardy | * Dla producenta sprzętu należy dostarczyć certyfikat: * ISO 9001 * ISO 14001 * ISO 50001 * Komputer spełniający: * ENERGY STAR 8.0 * Mil-STD-810H * Ochronę oczu TÜV Low Blue Light * Deklaracja zgodności CE (załączyć do oferty) * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki * Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy (IDLE) wynosząca maksymalnie 20 dB (załączyć dokument producenta komputera potwierdzający głośność) |
|  | Waga/Wymiary | Waga urządzenia z akumulatorem: 1,8 kg  Grubość notebooka nie większa niż: 19 mm |
|  | System operacyjny | system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1.Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN  e. Certyfikat/Klucz i uwierzytelnienie biometryczne  39.Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |
|  | Oprogramowanie do aktualizacji sterowników | Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. |
|  | Gwarancja | Minimalny czas trwania wsparcia technicznego producenta wynosi 12 miesięcy.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. |
|  | Wsparcie techniczne producenta | * Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera * Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00   Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. |

1. 8 komputerów stacjonarnych z monitorami

|  |  |  |
| --- | --- | --- |
| Lp. | Parametry | Wymagane minimalne parametry techniczne |
|  | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu. |
|  | Obudowa | Typu mini tower z obsługą kart PCI Express wyłącznie o wysokim (pełnym) profilu.  Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napedów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy.  Wyposażona w czytnik kart multimedialnych  - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym  - Wyposażona w budowany głośnik o mocy min. 2W |
|  | Zasilacz | Zasilacz maksymalnie 180W o sprawności minimum 85% |
|  | Chipset | Dostosowany do zaoferowanego procesora |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera.  Wyposażona w złącza min.:   * 1 x PCI Express 3.0 x16, * 1 x PCI Express 3.0 x1, * 2 x M.2 z czego min. 1 przeznaczona dla dysku SSD z obsługą PCIe NVMe |
|  | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi AMD Ryzen 5 5600G na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |
|  | Pamięć operacyjna | Min. 8GB DDR4 3200MHz z możliwością rozszerzenia do 64 GB  Ilość wolnych banków pamięci: min. 1 szt. |
|  | Dysk twardy | Min 256GB SSD M.2 PCIe NVMe zawierający recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
|  | Napęd optyczny | Nagrywarka DVD +/-RW |
|  | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci. |
|  | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. |
|  | Karta sieciowa | LAN 100/1000 Mbit/s z funkcją PXE oraz Wake on LAN  WiFi 802.11ac 2x2 + BT 5.0 |
|  | Porty/złącza | Wbudowane porty/złącza:  - 1 x VGA,  - 1 x HDMI,  - 8 x USB w tym min. 4 x USB3.2 z przodu komputera  - port sieciowy RJ-45,  - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy  - czytnik kart pamięci min. SD  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
|  | Klawiatura/mysz | Klawiatura przewodowa w układzie US  Mysz przewodowa (scroll) |
|  | System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN  e. Certyfikat/Klucz i uwierzytelnienie biometryczne  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI  - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:  - modelu komputera, PN  - numerze seryjnym,  - AssetTag,  - MAC Adres karty sieciowej,  - wersja Biosu wraz z datą produkcji,  - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni  - ilości pamięci RAM wraz z taktowaniem,  - stanie pracy wentylatora na procesorze  - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego)  Możliwość z poziomu Bios:  - wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy  - wyłączenia selektywnego (pojedynczego) portów SATA,  - wyłączenia karty sieciowej, karty audio, portu szeregowego,  - możliwość ustawienia portów USB w jednym z dwóch trybów:   1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer, ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej   - ustawienia hasła: administratora, Power-On, HDD,  - blokady aktualizacji BIOS bez podania hasła administratora  - załadowania optymalnych ustawień Bios  - obsługa Bios za pomocą klawiatury i myszy |
|  | Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:   * wykonanie testu pamięci RAM * test dysku twardego lub SSD * test monitora * test magistrali PCI-e * test portów USB * test płyty głównej * test myszy i klawiatury * test procesora   Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.  Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:   * PC: Producent, model * BIOS: Wersja oraz data wydania Bios * Procesor: Nazwa, taktowanie * Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci * Dysk: model, numer seryjny, wersja firmware, pojemność, temperatura pracy * Monitor: producent, model, rozdzielczość   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
|  | Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty) * Deklaracja zgodności CE (załączyć do oferty)   - Głośność jednostki mierzona z pozycji operatora w trybie IDLE nie większa niż 23 dB – dołączyć dokument potwierdzający głośność jednostki   * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki |
|  | Waga/rozmiary urządzenia | Wysokość nie może być większa niż 35cm  Szerokość nie może być większa niż 15cm |
|  | Bezpieczeństwo i zdalne zarządzanie | Złącze typu Kensington Lock |
|  | Gwarancja | 3 lata świadczona w miejscu użytkowania sprzętu (on-site)  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
|  | Wsparcie techniczne producenta | * Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera * Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. * Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera * Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00   Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. |
| MONITOR | | |
|  | Monitor | Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację monitora |
|  | Wielkość ekranu | Przekątna ekranu min. 23,8” |
|  | Matryca | Powłoka matrycy o wykończeniu matowym |
|  | Nominalna rozdzielczość | rozdzielczość nie mniejsza niż: FHD (1920x1080) |
|  | Kąty widzenia | Kąty widzenia min. 170 stopni w pionie i min. 170 stopni w poziomie |
|  | Plamka | Wielkość plamki (pojedynczego piksela) nie większa niż – 0.275 mm |
|  | Zakres kolorów | Nie mniejszy niż 72% (CIE 1931) |
|  | Kontrast | Kontrast wyświetlacza nie mniejszy niż: 3000:1  Jasność nie mniejsza niż 250 cd/m2 |
|  | Porty/złącza | Minimalna ilość dostępnych złącz monitorze:   * 1x HDMI * 1x VGA * 1x wyjście dźwięku |
|  | Kable/przejściówki | Do monitora producent dołącza minimum kable:   * HDMI * Kabel zasilający |
|  | Stopa/Podstawa monitora | Musi umożliwiać:  przechylenie w pionie min. 25 stopni ( -5 / 20 ) |
|  | Obudowa | * musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) * Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100) * Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora * Obudowa trwale oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikacje zaoferowanego monitora |
|  | Bezpieczeństwo | Złącze typu Kensington Lock |
|  | Zasilacz | Zasilacz wbudowany w obudowę monitora |
|  | Certyfikaty i standardy | - Certyfikat EPEAT na poziomie co najmniej Gold.  - ENERGY STAR  - TUV (min. Eye Comfort)  - TCO 8.0 lub wyższy  - TCO Edge 2.0 lub wyższy |
|  | Gwarancja | Min. 3 lata |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  - możliwość weryfikacji na stronie producenta modelu monitora  - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji  - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego |

1. 4 zasilacze awaryjne UPS do komputerów stacjonarnych

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Wymagane minimalne parametry techniczne** |
| 1 | Zastosowanie | Zasilacz awaryjny do komputerów stacjonarnych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji u producenta. |
| 2 | Moc | Minimum 600VA 360W |
| 3 | Zabezpieczenia | Zabezpieczenie przed przeładowaniem  Zabezpieczenie przeciwprzepięciowe |
| 4 | Komunikacja | USB  RJ11 |
| 5 | Napięcie wejściowe | 220/230/240 Vac |
| 6 | Częstotliwość wyjściowa | 50Hz lub 60Hz (automatyczne wykrywanie) |
| 7 | Baterie | Min. 1 x 12V/7Ah |
| 8 | Gniazda | Min. 2x Schuko |
| 9 | Czas reakcji | typowy 2-6 ms (maksymalny 10 ms) |
| 10 | Gwarancja | Min. 24 miesiące (min. 12 miesięcy na baterię) |
| 11 | Inne | Wskaźnik LCD |
| 12 | Uruchomienie i konfiguracja | Uruchomienie w siedzibie zamawiającego dostarczonego sprzętu w celu przetestowania poprawności działania |

1. 1 zasilacz awaryjny do serwerów

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Wymagane minimalne parametry techniczne** |
| 1 | Moc wyjściowa (pozorna / czynna | minimum 1650 VA  minimum 1650 W |
| DANE OGÓLNE I ŚRODOWISKOWE | | |
| 2 | Topologia | VI (line interactive) |
| 3 | Typ obudowy | Rack / Tower |
| 4 | Chłodzenie | Wymuszone, wewnętrzne wentylatory |
| WEJŚCIE | | |
| 5 | Napięcie znamionowe (wartość skuteczna) | 230 V AC |
| 6 | Zakres napięcia wejściowego (wartości skuteczne) i tolerancja | 178 ÷ 281 V AC ± 2 % |
| 7 | Częstotliwość znamionowa napięcia wejściowego | 50 Hz |
| 8 | Zakres częstotliwości i tolerancja | 45 ÷ 55 Hz ± 1 Hz |
| 9 | Progi przełączania: sieć – UPS | 178 ÷ 281 V AC ± 2 % |
| WYJŚCIE | | |
| 10 | Napięcie znamionowe (wartość skuteczna) | 230 V AC |
| 11 | Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa | 195 ÷ 253 V AC ± 2 % |
| 12 | Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa | 230 V AC ± 5 % |
| 13 | Automatyczna regulacja napięcia (AVR) | ± 10 % |
| 14 | Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) | Sinusoidalny / Tak jak na wejściu |
| 15 | Częstotliwość znamionowa napięcia wyjściowego | 50 Hz |
| 16 | Filtracja napięcia wyjściowego | Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy |
| 17 | Progi przełączania: UPS – sieć | 183 ÷ 276 V AC ± 2 % |
| 18 | Czas przełączenia na pracę rezerwową | < 3 ms |
| 19 | Czas powrotu na pracę sieciową | 0 ms |
| 20 | Przeciążalność | > 105% - 15 s (wyłączenie UPS) |
| AKUMULATORY I CZASY PODTRZYMANIA | | |
| 21 | Akumulatory wewnętrzne | minimum 12 V / 7 Ah VRLA |
| 22 | możliwość podłączenia zewnętrznego modułu bateryjnego | wymagane |
| 23 | Czas podtrzymania z baterii wewnętrznych lub przy wykorzystaniu zewnętrznego modułu bateryjnego dla obciążenia 1500W | minimum 15 min |
| PARAMETRY MECHANICZNE | | |
| 24 | Wymiary | wysokość zestawu nie większa niż 5U, głębokość nie większa niż 500 mm |
| ZABEZPIECZENIA | | |
| 25 | Zabezpieczenie wejściowe | Przeciwzwarciowe – Bezpiecznik automatyczny  16 A / 250 V AC  Przeciwprzepięciowe |
| 26 | Zabezpieczenie wyjściowe | Elektroniczne – przeciwzwarciowe i przeciążeniowe |
| 27 | Zabezpieczenia wejścia DC (akumulatory wewnętrzne) | Zabezpieczenie nadprądowe |
| WYPOSAŻENIE I FUNKCJE DODATKOWE | | |
| 28 | Przyłącza wyjściowe (liczba i typ gniazd) | minimum 8 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym) |
| 29 | Sygnalizacja | Akustyczno – optyczna; graficzny wyświetlacz LCD |
| 30 | Interfejsy komunikacyjne | USB HID, SNMP/HTTP |
| 31 | Gniazdo na dodatkowe karty rozszerzeń | wymagane |
| 32 | Wsporniki do montażu w szafie RACK | wymagane |
| 33 | Oprogramowanie monitorująco-zarządzające | * oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS * możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP) * możliwość zdalnego wyłączenia zarządzalnej sekcji gniazd * wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów * wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |
| 34 | Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego | wymagane |
| 35 | Możliwość aktualizacji oprogramowania firmware przez użytkownika | wymagane |
| GWARANCJA / SERWIS | | |
| 36 | Gwarancja | min 36 miesięcy na elektronikę i 24 miesiące na akumulatory; |
| 37 | Serwis | autoryzowany serwis producenta zlokalizowany w Polsce.  serwis realizowany w systemie door to door  naprawa w maksymalnie 5 dni roboczych |
| ZASTOSOWANE STANDARDY | | |
| 38 | Deklaracje | CE |
| 39 | Normy | PN-EN 62040-1:2009, PN-EN 62040-2:2008 |
| 40 | DODATKOWE OŚWIADCZENIA/DOKUMENTY | * ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań * oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji * karta katalogowa oferowanego sprzętu |
| 41 | Sposób montażu | Zasilacz oraz moduł bateryjny musi być wyposażony w zestaw szyn montażowych do montażu w szafie Rack 800-1200 mm |

1. 1 przełącznik zarządzalny

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Wymagane minimalne parametry techniczne** |
| 1 | Zastosowanie | Do zarządzania siecią lokalną. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji u producenta. |
| 2 | Ilość portów | Min. 24x 10/100/1000Base-T RJ45 + 4x 100/1000Base-X SFP |
| 3 | Matryca Przełączająca | Min. 55 Gb/s |
| 4 | Przepustowość | Min. 402Mp/s |
| 5 | Dodatkowe wymagania | Tablica adresów MAC współdzielona dla unicast i multicast (w proporcji 1:1)  Funkcje podwyższonej dostępności:  IEEE 802.1D STP, 802.1w RSTP, 802.1s MSTP, IEEE 802.3ad LACP, Virtual Cable Testing, Loop guard  Kontrola Ruchu:  802.1Q 4K VLAN, Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN, Voice VLAN, Mac VLAN, LACP algorytm adresu IP/MAC źródłowego/docelowego (load balance), GVRP, 802.1ad Vlan Stacking (QinQ)  Bezpieczeństwo:  Layer 2 MAC filtering, BPDU Tunnel, Uwierzytelnienie I autoryzacja logowania poprzez RADIUS and TACACS+, SSH v1/v2, DHCP/DHCPv6 snooping, IP/IPv6 Source Guard, Port security  QoS:  802.1p - 8 Priority Queues per Port, 802.1p Queuing method, Trusted COS/TOS/IP Precedence/DSCP/Port number, Broadcast Storm Control, Rate Limiting, port based, Strict priority, |
| 6 | Zarządzanie | Port konsolowy RS-232 (RJ45), GUI (Web), SNMP v1/v2c/v3, TFTP/FTP, Kopia zapasowa konfiguracji oraz jej przywracanie, Wielopoziomowy CLI, SNTP / NTP, Port Mirroring per IP/TCP/UDP |
| 7 | Instalacja i konfiguracja | Konfiguracja sieci, portów, sieci VLAN według zaleceń zamawiającego. |
| 8 | Gwarancja | Min. 24 miesiące |

1. 2 urządzenia do ochrony połączenia internetowego z licencją na 12 miesięcy na potrzeby szkół

|  |  |
| --- | --- |
| L.p. | Opis |
| OBSŁUGA SIECI | |
| 1 | Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP. |
| ZAPORA KORPORACYJNA (Firewall) | |
| 2 | Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. |
| 3 | Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. |
| 4 | Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). |
| 5 | Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. |
| 6 | Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. |
| 7 | Administrator ma możliwość zdefiniowania minimum 5 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u. |
| 8 | Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). |
| 9 | Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). |
| INTRUSION PREVENTION SYSTEM (IPS) | |
| 10 | System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. |
| 11 | Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. |
| 12 | Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. |
| 13 | Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. |
| 14 | Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. |
| 15 | Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. |
| 16 | Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. |
| KSZTAŁTOWANIE PASMA (Traffic Shapping) | |
| 17 | Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. |
| 18 | Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. |
| 19 | Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). |
| 20 | Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. |
| OCHRONA ANTYWIRUSOWA | |
| 21 | Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). |
| 22 | Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. |
| 23 | Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. |
| 24 | Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. |
| OCHRONA ANTYSPAM | |
| 25 | Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). |
| 26 | Ochrona antyspam ma działać w oparciu o:  a. białe/czarne listy,  b. DNS RBL,  c. heurystyczny skaner. |
| 27 | W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. |
| 28 | Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. |
| WIRTUALNE SIECI PRYWANTE (VPN) | |
| 29 | Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). |
| 30 | Odpowiednio kanały VPN można budować w oparciu o:   * 1. PPTP VPN,   2. IPSec VPN,   3. SSL VPN |
| 31 | SSL VPN musi działać w trybach Tunel i Portal. |
| 32 | W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. |
| 33 | Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). |
| 34 | Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. |
| FILTR DOSTĘPU DO STRON WWW | |
| 35 | Urządzenie ma posiadać wbudowany filtr URL. |
| 36 | Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. |
| 37 | Administrator musi mieć możliwość dodawania własnych kategorii URL. |
| 38 | Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. |
| 39 | Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. |
| 40 | Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:   1. blokowanie dostępu do adresu URL, 2. zezwolenie na dostęp do adresu URL, 3. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. |
| 41 | Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. |
| 42 | Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. |
| 43 | Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. |
| 44 | Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. |
| 45 | Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. |
| 46 | Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. |
| UWIERZYTELNIANIE | |
| 47 | Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:   * 1. lokalną bazę użytkowników (wewnętrzny LDAP),   2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),   3. usługę katalogową Microsoft Active Directory. |
| 48 | Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. |
| 49 | Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia  autoryzacje w oparciu o protokoły:   * 1. SSL,   2. Radius,   3. Kerberos |
| 50 | Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. |
| 51 | Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. |
| 52 | Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. |
| ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP) | |
| 53 | Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). |
| 54 | Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:   * 1. równoważenie względem adresu źródłowego,   2. równoważenie względem połączenia |
| 55 | Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. |
| 56 | Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |
| 57 | Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. |
| 58 | Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |
| 59 | Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. |
| 60 | Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. |
| POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA | |
| 61 | Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. |
| 62 | Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. |
| 63 | Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. |
| 64 | Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS |
| 65 | Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. |
| 66 | Urządzenie musi posiadać usługę DNS Proxy. |
| ADMINISTRACJA URZĄDZENIEM | |
| 67 | Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. |
| 68 | Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. |
| 69 | Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. |
| 70 | Komunikacja może odbywać się na porcie innym niż https (443 TCP). |
| 71 | Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. |
| 72 | Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. |
| 73 | Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. |
| 74 | Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). |
| 75 | Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. |
| 76 | Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. |
| RAPORTOWANIE | |
| 77 | Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. |
| 78 | System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. |
| 79 | System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. |
| 80 | System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. |
| 81 | System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. |
| 82 | W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. |
| 83 | Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy |
| PARAMETRY SPRZĘTOWE | |
| 84 | Urządzenie nie musi być wyposażone w dysk twardy, oprogramowanie wewnętrzne może działać z wbudowanej pamięci flash. |
| 85 | Liczba portów Ethernet 10/100/1000Mbps – min. 8. |
| 86 | Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. |
| 87 | Przepustowość Firewalla – min. 3,5 Gbps |
| 88 | Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps. |
| 89 | Przepustowość filtrowania Antywirusowego – min. 400 Mbps |
| 90 | Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100. |
| 91 | Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. |
| 92 | Obsługa min. VLAN 64 |
| 93 | Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę. |
| 94 | Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. |
| 95 | Urządzenie nie może być limitowane na użytkowników. |

1. 1 dysk sieciowy NAS do archiwizacji danych

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Wymagane minimalne parametry techniczne** |
| 1 | Procesor | czterordzeniowy |
| 2 | Pamięć RAM | Min. 2GB DDR4 |
| 3 | Przechowywanie | Min. 4 kieszenie na dyski,  Dyski 4x 4TB SATA HDD – dedykowane do pracy w serwerach NAS |
| 4 | Porty zewnętrzne | Port LAN RJ-45 1GbE 4szt. (z obsługą funkcji Link Aggregation)  Min. 2x USB 3.0  Port Seata 1 szt. |
| 5 | Inne | Wentylator w obudowie ( 3 tryby pracy, pełnej prędkości, chłodzenia, cichy)  Kontrolki LED z regulacją jasności  Funkcja przywracania zasilania  Funkcja planowania włączenia/wyłączenia  Funkcja Wake on LAN/WAN |
| 6 | Dodatkowe wymagania | W komplecie jednostka główna, zasilacz, kabel zasilania x1, kabel LAN Rj45 x1 |
| 7 | Oprogramowanie | Zarządzanie przechowywaniem:  - obsługiwane tryby macierzy: RAID 0, 1, 5, 6, 10,  - protokół plików: SMB/AFP/NFS/FTP/FTPS  - serwer SYSLOG - liczba zdarzeń na sekundę: min. 800  - protokoły sieciowe: SMB1 (CIFS), SMB2, SMB3, HTTP, HTTPs, FTP, SNMP,  Oprogramowanie w języku polskim. |
| 8 | Uruchomienie i konfiguracja | Uruchomienie w siedzibie zamawiającego dostarczonego sprzętu w celu przetestowania poprawności działania. Zamontowanie dysków, testy działania. |
| 9 | Gwarancja | Min. 24 miesiące |

1. 1 skaner dokumentów do elektronicznego obiegu dokumentów

|  |  |
| --- | --- |
| Lp. | Wymagane minimalne parametry techniczne |
| 1. | Skaner dokumentów do elektronicznego obiegu dokumentów. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji u producenta. |
| 2. | Automatyczne skanowanie dwustronne |
| 3. | Prędkość skanowania 40 str./min / 80 obr./min w kolorze, skali szarości i trybie monochromatycznym |
| 4. | Automatyczny podajnik dokumentów (ADF) na 80 arkuszy |
| 5. | Wbudowany podajnik płaski (216 mm x 297 mm) |
| 6. | Źródło światła LED |
| 7. | Pakiet Scanner Central Admin Suite |
| 8. | Skanowanie wypukłych kart (1,4 mm grubości) |
| 9. | W zestawie PaperStream IP (TWAIN/ISIS) i PaperStream Capture |
| 10. | Maksymalny format dokumentu 216 x 356 mm |
| 11. | Rozdzielczość optyczna 600 dpi |
| 12. | Głębia kolorów (wejście / wyjście) 24-bit / 24-bit |
| 13. | Skala szarości (wejście / wyjście) 8-bit / 8-bit |
| 14. | Formaty plików: PDF, JPEG, TIFF, BMP |
| 15. | Gwarancja min. 12 miesięcy |