

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

ZPI.271.1.8.2022

Załącznik nr 1 do SWZ

**Szczegółowy opis przedmiotu zamówienia - OPZ**

**ZADANIE NR 1:**

**Specyfikacja serwera wraz z oprogramowaniem szt. 1:**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | Zainstalowane dwa procesory 8-rdzeniowe, klasy x86, dedykowane do pracy z zaoferowanym serwerem, taktowane zegarem min. 2.8 GHz (częstotliwość bazowa) umożliwiające osiągnięcie wyniku minimum 34 500 punktów w teście PassMark dla konfiguracji Dual CPU- CPU Mark dostępnym na stronie internetowej: <https://www.cpubenchmark.net/multi_cpu.html> z dnia 10.08.2022 (wyniki załączone do dokumentów zapytania). |
| **RAM** | Minimum 256GB DDR4 RDIMM 3200MT/s w kościach 16GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing |
| **Gniazda PCI** | - minimum jeden slot PCIe x16 oraz minimum dwa sloty PCIe x8 generacji 4 |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSD  Zainstalowane 4 dyski SSD SAS o pojemności min. 1.92 TB, 6Gb/s, Hot-Plug o parametrze DWPD wynoszącym min. 1.  Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |
| **System operacyjny/System wirtualizacji** | Dwie licencje na system Windows Server 2022 Standard, każda licencja pokrywająca wszystkie fizyczne rdzenie w serwerze.  Licencje muszą umożliwić uruchomienie 4 maszyn wirtualnych na oferowanym serwerze.  System należy dostarczyć wraz z licencjami CAL na 35 użytkowników oraz licencjami na usługi zdalnego pulpitu dla 5 użytkowników. |
| **Wbudowane porty** | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,  Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | Redundantne, Hot-Plug min. 800W każdy. |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| **Diagnostyka** | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * integracja z Active Directory; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera * możliwość obsługi przez sześciu użytkowników jednocześnie; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.  Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows Server 2022. |
| **Warunki gwarancji** | 5 lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

1. Zadanie obejmuje migracja struktury serwera 1:1 z aktualnie działającego systemu Windows Server 2012 R2 opartej na Hyper – V łącznie z maszynami wirtualnymi (dane, oprogramowanie robocze) na dostarczane urządzenie.
2. Zadanie obejmuje również przeprowadzenie testów prawidłowego działania oprogramowania roboczego między serwerem a stanowiskami roboczymi.

**UPS - Zasilacz awaryjny specyfikacja szt. 1:**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa elementu, parametru lub cechy | Opis wymagań |
| 1 | Moc pozorna | 2200 VA |
| 2 | Moc rzeczywista | 2200 W |
| 3 | Współczynnik mocy | 1 |
| 4 | Topologia (klasyfikacja IEC 62040-3) | podwójna konwersja on-line |
| 5 | Typ obudowy | Uniwersalna tower/rack |
| 6 | Liczba, typ gniazd wyjściowych | 8 x C13, 2 x C19. |
| 7 | Typ gniazda wejściowego | Gniazdo C20 |
| 8 | Czas podtrzymania dla obciążenia mocą 1,8 kW z zastosowaniem 2 dodatkowych modułów bateryjnych | 57 minut |
| 9 | Napięcie znamionowe | 230 V |
| 10 | Tolerancja napięcia prostownika | 176 - 276 V (do 100 - 276 V przy obciążeniu <33%) |
| 11 | Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| 12 | Tolerancja częstotliwości | 40 - 70 Hz |
| 13 | Napięcie znamionowe wyjściowe | 230 V (domyślnie) / 200/208/220/240 V |
| 14 | Częstotliwość wyjściowa | 50/60 Hz |
| 15 | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| 16 | Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| 17 | Ochrona przed głębokim rozładowaniem | Tak |
| 18 | Okresowy automatyczny test baterii | Tak (standardowo co tydzień) |
| 19 | Zimny start | Tak |
| 20 | System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| 21 | Interfejs komunikacyjny | • USB |
| • RS232 DB-9 żeński (HID) |
| • miniport wyłącznik awaryjny RPO |
| • miniport wyłącznik ON/OFF |
| • listwa zaciskowa dla przekaźnika wyjściowego |
| 22 | Panel sterowania z wyświetlaczem LCD | • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS’a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh) |
|  | • Poziomy rząd przycisków sterowania |
|  | • Poziomy rząd wskaźników stanu: trybu online (zielony), trybu bateryjnego (pomarańczowy), trybu bypass (pomarańczowy), usterki (czerwony) |
| 23 | Przyciski sterujące i wskaźniki diodowe LED | • sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie) |
| • przycisk Escape (anulowanie) |
| • przyciski funkcyjne (przewijanie w górę i w dół) |
| • przycisk Enter (potwierdzający) |
| 24 | Wyposażenie | •  UPS 2,2 kVA, instrukcja obsługi, instrukcja bezpieczeństwa |
| •  przewód zasilający |
| •  kabel RS232 |
| •  kabel USB |
| •  karta SNMP |
| •  uchwyty kablowe |
| •  podstawki do montażu pionowego (wieża) |
| •  2 przewody IEC 10 A |
| •  zestaw szyn montażowych do szafy 19" |
| 25 | Karta SNMP | • cyberbezpieczeństwo (certyfikaty UL 2900-2-2/IEC62443/HTTPS/MQTT/ /RNDIS/LDAP/NVD//SSH/PKI, pakiet szyfrów TLS 1.2 z minimum SHA256) |
| • certyfikaty CA i PKl |
| • prędkość gigabit’owa (half-duplex, full-duplex) |
| • różne poziomy nadawania dostępu do konta administratora lub użytkownika |
| 26 | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii (minimum: Windows: 2000, XP, 2003, Vista, Server 2008, 7, 10; Linux: Red Hat, Fedora Core, SuSE; UNIX: AIX, HP-UX, SCO, SGI Irix, Mac OS, Sun Solaris). Oprogramowanie musi mieć możliwość wyboru polskiej wersji językowej. |
| 27 | Maksymalna wysokość UPS wraz z modułami bateryjnymi | 6U |
| 28 | Poziom hałasu w odl. 1m | < 47 dBA |
| 29 | Zgodność z normami UE | Deklaracja zgodności producenta |
| 30 | Dodatkowe cetyfikaty | ISO9001 producenta urządzenia |
| 31 | Gwarancja producenta | 36 miesięcy dla elektroniki, 24 miesięcy dla baterii |

1. Zadanie obejmuje również podłączenie oraz konfigurację UPS z nowym systemem.

**Specyfikacja macierzy dyskowej szt. 1:**

|  |  |
| --- | --- |
| Procesor | Jeden 4-rdzeniowy/4-wątkowy Intel Celeron N5105/N5095 lub równoważny procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4000 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net |
| Obudowa | Rack 2U o wymiarach nie większych niż, 87× 483 × 320 mm  (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK |
| Pamięć RAM | 4 GB SODIMM DDR4  Urządzenie powinno obsługiwać do 16GB pamięci RAM. |
| Ilość obsługiwanych dysków | 8 dysków 3,5-calowych 3,5/2,5 dyski SATA |
| Zamontowane dyski twarde | Osiem dysków twardych o pojemności 8TB każdy znajdujące się na liście kompatybilności producenta oferowanego urządzenia NAS spełniające wymagania: SATA 6 Gb/s, 3,5”, 256MB pamięci podręcznej, 7200 obr./min, MTBF min 2000000 h, Czujnik wilgotności, gwarancja producenta 5 lat |
| Interfejsy sieciowe | 2 porty 2,5Gigabit sieci Ethernet (RJ45) |
|  |
| Porty | 2 gniazda typu A USB 2.0  2 gniazda typu A USB 3.2 Gen 2 10 Gb/s  1 gniazdo HDMI 1.4b |
| Porty PCIe | Co najmniej:  1x gniazdo Gen3 x2 |
| Wskaźniki LED | Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej |
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60 |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych. |
| System Operacyjny | Apple Mac OS 10.10 lub nowszy  Linux and UNIX  Microsoft Windows 7, 8, 10 i 11  Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 I 2019 |
| Stacja monitoringu | Tak, w standardzie 8 darmowych licencji na podłączenie kamer. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu  Windows ACL  Integracja w Windows ADS  Serwer WWW  Serwer plików  Manager plików przez WWW  Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI  Replikacja w czasie rzeczywistym  Serwer RADIUS  Klient LDAP  Serwer Syslog  Container Station |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Gwarancja i serwis | 36 miesięcy gwarancji na macierz oraz 5 lat gwarancji na dyski twarde |
| Waga | Nie więcej niż 7 kg (netto) |
| System plików | Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Liczba kont użytkowników | 4096 |
| Liczba grup | 512 |
| Liczba udziałów | 512 |
| Max ilość połączeń (CIFS) | 1500 |
| Zasilanie | 300W, 100–240 V |
| Wentylatory | 2 x 80mm, 12VDC |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |

1. Zadanie obejmuje również podłączenie i konfigurację automatycznej kopii zapasowej systemu oraz baz danych.

**UTM zarządzalny szt. 1:**

**Wymagania Ogólne**

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

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

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall.

• Ochrony w warstwie aplikacji.

• Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

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

3. Monitoring stanu realizowanych połączeń VPN.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

4. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.

4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 600 Mbps.

**Funkcje Systemu Bezpieczeństwa:**

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL.

**Polityki, Firewall**

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

2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

• Translację jeden do jeden oraz jeden do wielu.

• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

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

4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

• Amazon Web Services (AWS).

• Microsoft Azure

• Cisco ACI.

• Google Cloud Platform (GCP).

• OpenStack.

• VMware vCenter (ESXi).

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

• Wsparcie dla IKE v1 oraz v2.

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

• Obsługa protokołu Diffie-Hellman grup 19 i 20.

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

• Routingu statycznego.

• Policy Based Routingu.

• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

**Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

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

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Opisy do wymagań ogólnych**

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

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

1. Zadanie obejmuje przeniesienie pełnej konfiguracji obecnie działającego urządzenia Fortigate 60D łącznie z ustawieniami VPN oraz wszystkim podsieciami na dostarczane urządzenie.
2. Zadanie obejmuje również przetestowanie poprawności działania.

**Switch zarządzalny szt. 3:**

Przełącznik sieciowy

1. Parametry fizyczne platformy:

• wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U

• Zasilanie 230V

• MTBF > 10lat

2. Interfejsy sieciowe – wymagania minimalne:

• 48 portów GE, RJ-45

• 4 porty 10GE SFP+

3. Zarządzanie:

• port konsoli szeregowej RJ45

• Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę

• Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall)

• Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.

• Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników

• Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).

• Kontroler musi oferować możliwość automatycznej instalacji wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika. Oprogramowanie przełącznika, musi być przechowywane na kontrolerze.

4. Parametry wydajnościowe:

• przepustowość urządzenia - min. 176 Gbps, min. 260 Mbps

• możliwość zapamiętania co najmniej 32 000 adresów MAC

• Opóźnienie - poniżej 1 mikrosekundy

• Bufor pakietów: min. 2 MB

• Pamięć DRAM: min. 512 MB

• Pamięć FLASH: min. 64 MB

5. Wymagane funkcje:

• możliwość automatycznej negocjacji prędkości i duplexu dla połączeń

• obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)

• możliwość agregacji portów zgodna z 802.3ad

• obsługa co najmniej 4000 VLANów, zgodna z 802.1Q • możliwość wykonywania routingu statycznego (realizowany software’owo)

• port-mirroring

• Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius

• zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)

• możliwość zarządzania przez interfejs graficzny i tekstowy

• możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI

• możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:

- możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników

- obsługa białych i czarnych list MAC

- stateful firewall, umożliwiający kontrolę dostępu do sieci

- routing statyczny i dynamiczny, co najmniej OSPF

6. Gwarancja oraz wsparcie:

• Dożywotnia Gwarancja: urządzenia muszą być objęte dożywotnią producenta, gwarantującą wymianę wadliwego sprzętu (okres 5 lat od ogłoszenia zakończenia produkcji).

• Wsparcie serwisowe: System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

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

• Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

1. Zadanie obejmuje również podłączenie i konfigurację nowo dostarczonych urządzeń.

**ZADANIE NR 2:**

**Zakup komputerów przenośnych szt. 2:**

|  |  |
| --- | --- |
| Nazwa | Wymagane parametry techniczne (minimalne) |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Matryca | Matryca o przekątnej 15.6” z powłoką przeciwodblaskowa i rozdzielczością 1920 x 1080. Jasność matrycy 250 cd/m2, kontrast min. 700:1 |
| Procesor | Procesor dedykowany do pracy w laptopach, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 10180 punktów według wyników opublikowanych na stronie <https://www.cpubenchmark.net/laptop.html>  **z dnia 10.08.2022 (wyniki załączone do zapytania)** |
| Pamięć RAM | 8GB DDR4 3200MHz możliwość rozbudowy do min 32GB, min. jeden wolny slot pamięci na dalszą rozbudowę |
| Pamięć masowa | Min. 512GB SSD NVMe  Fabrycznie dostosowane miejsce do instalacji drugiego dysku SATA 2,5” |
| Karta graficzna | Zintegrowana z procesorem |
| Klawiatura | Klawiatura w układzie US - QWERTY z wydzieloną klawiaturą numeryczną oraz z wbudowanym w klawiaturze podświetleniem. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2 x 2W.  Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.  Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę.  Czytnik kart multimedialnych w formacie microSD,  Złącze audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Karta Wireless AX 2x2 + Bluetooth 5.1 |
| Bateria i zasilanie | Min. 54 Wh umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.  Zasilacz o mocy min. 65W |
| Waga | Waga max 2 kg z baterią |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, uszczelnienie dookoła matrycy chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni.  Komputer spełniający normy MIL-STD-810H (załączyć oświadczenie producenta) |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego (wmontowanego na stałe). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i maks osiąganej prędkości, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag, nie podlegające skasowaniu nawet po aktualizacji BIOS.  Funkcja logowania się do BIOS na podstawie hasła użytkownika i administratora (hasła niezależne), możliwość ustawienia haseł administratora oraz użytkownika składających się z małych liter, dużych liter, cyfr, znaków specjalnych.  BIOS zawierający informację o stanie naładowania baterii, mocy podpiętego zasilacza, ponadto możliwość zarządzania trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
| Certyfikaty | Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty)  Certyfikat ISO 50001 dla producenta sprzętu (należy załączyć do oferty)  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  Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony)  Certyfikat EPEAT min. Silver dla Polski |
| Diagnostyka | 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 i dodatkowych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.  Czytnik linii papilarnych |
| System operacyjny | Zainstalowany system operacyjny Windows 10 Professional |
| Oprogramowanie dodatkowe | Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające :  - określenie preferencji aktualizacji  - ustawienie priorytetu aktualizacji  - użycia opcji planowania aktualizacji bieżących wersji sterowników,  Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :  - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :                  a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja                  f.  wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.  - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )  - dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
| Porty i złącza | Wbudowane porty i złącza: 1 x HDMI 1.4, 1x RJ-45, 1 x USB 2.0, 2 x USB 3.2 typu A, w tym jeden dosilony, 1x USB 3.2 gen 2 typu C, port zasilania, 1 x RJ-45, gniazdo linki zabezpieczającej. |
| Wsparcie techniczne | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) |
| Warunki gwarancyjne | 3-letnia gwarancja producenta świadczona na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem  W przypadku awarii dysku twardego uszkodzony dysk zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) |

**Zakup komputerów przenośnych szt.4:**

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Zastosowanie** | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej, |
| **Matryca** | Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED matryca matowa, jasność min. 220nits, kontrast 400:1 |
| **Wydajność** | Procesor dedykowany do pracy w laptopach, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 10050 punktów według wyników opublikowanych na stronie <https://www.cpubenchmark.net/laptop.html>  **z dnia 10.08.2022 (wyniki załączone do zapytania)** |
| **Pamięć RAM** | 8GB DDR4 możliwość rozbudowy do min 16GB, dwa sloty pamięci dostępne dla użytkownika (nie dopuszcza się pamięci wlutowanych); możliwość rozbudowy pamięci przez użytkownika, bez kontaktu z serwisem producenta. |
| **Pamięć masowa** | min. 256 GB SSD NVMe, fabryczna możliwość instalacji drugiego dysku 2,5” |
| **Karta graficzna** | Zintegrowana z procesorem |
| **Multimedia** | Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy min. 2x 2W, cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.  Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze. |
| **Bateria i zasilanie** | Min. 41 Wh. Zasilacz o mocy min. 65W |
| **Waga** | Waga komputera z oferowaną baterią nie większa niż 1,7kg |
| **Obudowa** | Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z wzmacnianego metalu. |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy.  BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej.  Funkcja blokowania/odblokowania portów USB  Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS’u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł/wy funkcji. Hasła silne opatrzone o litery, cyfry i znaki specjalne.  Możliwość przypisania w BIOS numeru nadawanego przez Administratora. |
| **Bezpieczeństwo** | System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT’owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego, braku dostępu do sieci LAN i internetu oraz nie może być realizowana przez narzędzia zewnętrzne podłączane do komputera (np. pamięć USB flash).  Dedykowany układ szyfrujący TPM 2.0  Złącze na linkę zabezpieczającą przed kradzieżą. |
| **Certyfikaty** | Certyfikat ISO 9001 dla producenta sprzętu (załączyć do oferty)  Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty)  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.  Certyfikat Energy Star lub TCO dla oferowanego modelu. |
| **System operacyjny** | Zainstalowany system operacyjny Windows 11 Professional |
| **Wymagania dodatkowe** | Wbudowane porty i złącza: HDMI 1.4, RJ-45 (karta sieciowa wbudowana), min. 3xUSB w tym min. 2 port USB 3.2 gen1 typ-A, czytnik kart SD 3.0, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB)  Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 4.1  Klawiatura (układ US - QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów, z wbudowanym podświetleniem |
| **Warunki gwarancji** | Min. 3-letnia gwarancja producenta świadczona na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów oraz sprawdzenie okresu gwarancji, fabrycznej konfiguracji.  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |

**ZADANIE NR 3:**

**Urządzenie wielofunkcyjne A3 szt.2:**

|  |  |
| --- | --- |
| **Specyfikacja urządzenia wielofunkcyjnego** | |
| Technologia druku | kolorowy druk laserowy, automatyczny druk dwustronny w standardzie |
| Technologia tonera | tonery CMYK wyprodukowane z wykorzystaniem składników naturalnych |
| Szybkość druku | minimum 25 stron/minutę |
| Czas oczekiwania na wydruk pierwszej strony kolorowej | maksymalnie 7 sek |
| Czas oczekiwania na wydruk pierwszej strony mono | maksymalnie 5,5 sek |
| Czas nagrzewania | do 14 sek. |
| Pamięć RAM | min 4GB |
| Dysk twardy | SSD 256 GB |
| Język wydruku | PCL 6 (XL3.0); PCL 5c; PostScript 3 (CPSI 3016); XPS |
| Rozdzielczość wydruku | 1,800 (equivalent) x 600 dpi; 1200 x 1200 dpi |
| Maksymalne obciążenie miesięczne | minimum 100 000 stron miesięcznie |
| Kopiowanie wielokrotne | 1-9999 |
| Powiększenie | 25–400 % w odstępach 0,1% |
| Funkcje kopiowania/drukowania | wstawianie rozdziałów, okładek i stron, kopia próbna (drukowana i ekranowa), druk próbny do regulacji, tryb plakatowy, powtarzanie obrazu, znak wodny, pieczętowanie, ochrona przed kopiowaniem, kopiowanie dokumentów tożsamości, bezpieczny wydruk, Pomijanie pustych stron, wydruk bannerowy, tworzenie ulotek, wstawianie obrazów |
| Możłiwość druku z USB | (DOCX, JPEG, PDF, compact PDF, PPML, PPTX, TIFF, VDX, XLSX, XPS, compact XPS, ZIP) |
| Pierwszy podajniki papieru | minimum 500 arkuszy (format A5 do A3) |
| Drugi podajnik papieru | minimum 500 arkuszy (format A5 do SRA3) |
| Podajnik papieru ręczny | minimum 150 arkuszy, A6-SRA3 |
| Dodatkowe podajniki papieru | Możliwość doposażenia o dodatkowe podajniki kaset w podstawie urzadzenia, rozbudowujące pojemność kaset papieru urządzenia do minimum 6650 arkuszy A4. |
| Podajnik oryginałów | 100 arkuszy, format oryginałów A6 - A3, podajnik z funkcją skanowania dwustronnego, |
| Pojemność odbiorcza | 250 arkuszy |
| Prędkość procesora | czterordzeniowy procesor min. 1,6 GHz |
| Prędkość skanowania | min 80 str/minutę |
| Rodzaj modułu skanera | wbudowany kolorowy skaner, z wbudowanym energooszczędnym oświetleniem w technologi LED |
| Rozdzielczość skanowania | 600 x 600 dpi |
| Tryby skanowania | Scan-to-USB, Scan-to-Me, Skan-to-SMB, Scan-to-Home, Scan-to-FTP, Scan-to-Box, Scan-to-USB, Scan-to-WebDAV, Scan-to-DPWS, Network TWAIN scan. Adnotacje (tekst/godzina/data) w plikach PDF; Pomijanie pustych stron. Podgląd i edycja zeskanowanych obrazów przed wysłaniem/zapisaniem. |
| Formaty plików | JPEG; TIFF; PDF; kompaktowy PDF; zaszyfrowany PDF; XPS Kompaktowy XPS; PPTX; PDF/A |
| Obsługiwane formaty papieru | A6–SRA3. Możlwiość druku na mediach 297 mm x 1200 mm |
| Obsługiwane formaty papieru w druku/kopiowaniu dwustronnym | A5-SRA3 |
| Obsługiwana gramatura papieru | 52 - 300 g/m2 |
| Obslugiwana gramatura papieru w druku/kopiowaniu dwustronnym | 52-300 g/m2 |
| Interfejsy | USB 2.0, złącze Ethernet 10Base-T / 100Base-TX / 1000Base-T, |
| Obsługiwane protokoły | Ethernet, Apple Talk, TCP/IP (IPv4, IPv6), HTTP / HTTPS, SSL/TSL for HTTPS, SMB, Port 9100 (dwu-kierunkowy), IPP, LDAP, SNMP V3 |
| Obsługiwane protokoły sieciowe | HTTP, TCP/IP (IPv4, IPv6), IPX/SPX (wsparcie ND), SMB (NetBEUI), LPD, IPP 1.1, SNMP |
| Wsparcie systemów operacyjnych | Windows 7 (32/64); Windows 8/8.1 (32/64)' Windows 10 (32/64) Windows Server 2008 (32/64), Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019; Macintosh OS X 10.10 or later; Unix/Linux/Citrix, SAP |
| Zasilanie | 220-240 V (±10%), 50/60 Hz (±2 Hz) |
| Wyświetlacz | kolorowy min 10-calowy pojemnościowy dotykowy wyświetlacz LCD, wraz w wbudowaną animowaną pomocą dla użytkownika, z możliwością zdalnej obsługi panelu uzytkownika przez przeglądarkę WWW. |
| Język menu | Polski |
| Inne | Możliwość podłączenia wewnętrznego czytnika zbliżeniowych kart identyfikacyjnych, wbudowanego w obudowę urządzenia |
| Inne funkcje urządzenia | Obsługa NFC w standardzie, z możliwością autoryzacji użytkowników. |
| Inne funkcje urządzenia | Wbudowana przeglądarka |
| Inne funkcje urządzenia | Obsługa Apple Airprint i Google Cloud Print |
| Inne funkcje urządzenia | Dodatkowa szuflada na dokumenty i materiały eksploatacyjne |
| Ekologia | Licznik czasu pracy urządzenia, licznik współczynika druku dwustronnego. Automatycznie dostosowujący się tryb oszczędzania energii. Parametr TEC poniżej 1 kWh/tydzień. |
| Certyfikaty | NEMKO, EMC, ISO 9001, ISO 14001, Blue Angel Mark, TUV |
| Oprogramowanie antywirusowe | Możliwość zainstalowania aplikacji antywirusowej bezpośrednio na urządzeniu. Antywirus powinien mieć funkcje skanowania w czasie rzeczywistym bądź na żądanie |
| Gwarancja | Minimum 24 miesiące |

1. Zadanie obejmuje również podłączenie oraz konfigurację drukarek zgodnie z aktualną konfiguracją obowiązującą w UMG.
2. Urządzenie musi zawierać komplet oryginalnych tonerów oraz oryginalną podstawę na kółkach, pochodzącą od producenta.

**Skaner szt. 1:**

|  |  |
| --- | --- |
| Specyfikacja skanera | |
| Typ skanera | Skaner z podajnikiem |
| Rozdzielczość skanowania | 600 DPI x 600 DPI |
| Formaty papieru | A4, A5, A6, B5, B6, Letter, Pocztówka, Wizytówki, plastikowe karty |
| Prędkość skanowania | Monochromatyczny 45 Str./min. – Kolor 45 Str./min/ |
| Pojemność | 100 arkusze |
| Dzienna wydajność | 5000 stron |
| Skanowanie dwustronne | Tak |
| Funkcje | Pomijanie pustych stron, Usuwanie otworów po dziurkaczu, automatyczna korekta położenia ukośnego, maskowanie nieostrości |
| Przyłącza | USB 3.0, Interfejs Ethernet (1000 Base-T/100-Base-TX/ 10-Base-T |
| Gwarancja | Minimum 24 miesiące |

1. Zadanie obejmuje również podłączenie I konfigurację dostarczanego sprzętu.