Załącznik nr 2
Specyfikacja techniczna

## CZĘŚĆ 1 – KOMPUTERY STACJONARNE, MONITORY, OPROGRAMOWANIE, LICENCJA;

**Komputer stacjonarny - 13 sztuk**

| Nazwa komponentu | Wymagane parametry techniczne komputerów |
|---|---|
| Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| Wydajność obliczeniowa | Procesor wielordzeniowy zintegrowanym z układem graficznym osiągający w teście wydajności CPU PassMark Performance Test co najmniej wynik 19400 punktów (https://www.cpubenchmark.net) z wynikiem aktualnym nie starszym niż na dzień publikacji ogłoszenia. |
| Pamięć RAM | 16 GB DDR4 3200MHz. Możliwość rozbudowy do min. 64GB. |
| Pamięć masowa | Dysk SSD 256GB PCIe NVMe<br>Dysk HDD 1 TB 3.5”. |
| Wydajność grafiki | Zintegrowana karta graficzna osiągająca w teście co najmniej wynik 1500 punktów (https://www.cpubenchmark.net) z wynikiem aktualnym nie starszym niż na dzień publikacji ogłoszenia. |
| Obudowa | Typu Small Form Factor. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej.<br>Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi |

| | |
|---|---|
| | sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Bezpieczeństwo | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.<br>Procedura POST traktowana jest jako oddzielna funkcjonalność. |
| BIOS | BIOS zgodny ze specyfikacją UEFI. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:<br>- wersji BIOS,<br>- numerze seryjnym komputera,<br>- ilości i prędkości zainstalowanej pamięci RAM, oraz sposobie obsadzeniu slotów pamięci<br>- pojemności zainstalowanego lub zainstalowanych dysków twardych<br>- funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)<br>-Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |

| | |
|---|---|
| System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Zainstalowana pełna, nieograniczona czasowo oraz legalna polska wersja systemu operacyjnego Microsoft Windows 11 Pro 64-bit - lub produkt równoważny o cechach równoważności określonych niżej*).<br><br>System musi być nowy (nie aktywowany wcześniej na innym urządzeniu). Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym. Nie dopuszcza się zaoferowania systemu operacyjnego typu refurbished. Nie jest dopuszczalne rozwiązanie w zakresie emulacji systemu operacyjnego.<br><br>*) Opis (cechy) równoważności dla systemu operacyjnego:<br>• umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;<br>• możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji;<br>• zapewniać internetową aktualizację w języku polskim;<br>• posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;<br>• posiadać interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim;<br>• posiadać budowany system pomocy w języku polskim;<br>• posiadać wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);<br>• posiadać graficzne środowisko instalacji i konfiguracji;<br>• mieć zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików;<br>• posiadać dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>o klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>o dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>• wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami;<br>• posiadać zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;<br>• możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci; |

| | |
|---|---|
| | • 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.);<br>• posiadać możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>• posiadać graficzne środowisko instalacji i konfiguracji dostępne w języku polskim;<br>• posiadać klucz produktu przypisany do komputera aby przy ponownej reinstalacji systemu nie było konieczności wpisywania klucza;<br>• posiadać 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;<br>• posiadać możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);<br>• posiadać funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>• mieć wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. |
| Certyfikaty i dokumenty | 1) oferowany sprzęt musi posiadać oznaczenie CE – dokumentem potwierdzającym spełnienie wymagań będzie załączona do oferty deklaracja zgodności CE producenta sprzętu.<br>2) potwierdzenie spełniania kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki odnoszącego się do zaoferowanego produktu |
| Dźwięk | Zintegrowana karta dźwiękowa |
| Złącza - panel przedni | USB 2.0 - 2 szt.<br>USB 3.2 Gen. 1 - 2 szt.<br>Wyjście słuchawkowe/wejście mikrofonowe - 1 szt.<br>Minimalna ilość złącz nie może być osiągnięta przy pomocy zewnętrznych HUB-ów lub przejściówek. |
| Złącza - panel tylny | USB 2.0 - 2 szt.<br>USB 3.2 Gen. 1 - 2 szt.<br>Wyjście słuchawkowe/głośnikowe - 1 szt. |

| | |
|---|---|
| | RJ-45 (LAN) - 1 szt.<br>HDMI - 1 szt.<br>Display Port - 1 szt.<br>AC-in (wejście zasilania) - 1 szt.<br>Minimalna ilość złącz nie może być osiągnięta przy pomocy zewnętrznych HUB-ów lub przejściówek. |
| Porty wewnętrzne (wolne) | PCI-e x16 - 1 szt.<br>PCI-e x1 - 1 szt. |
| Łączność | Wi-Fi 5 (802.11 a/b/g/n/ac)<br>LAN 10/100/1000 Mbps<br>Bluetooth |
| zasilacz | Tak |
| | Możliwość zabezpieczenia linką (port Kensington Lock)<br>Wbudowany moduł TPM |
| Wymagania dodatkowe | Klawiatura USB w układzie polski programisty<br>Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)<br>Wbudowana nagrywarka DVD +/-RW<br>Kabel zasilający |
| Wsparcie techniczne producenta | 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 gwarancji | Min. 2-letnia gwarancja producenta.<br>Czas reakcji serwisu - do końca następnego dnia roboczego<br>Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.<br>Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) |

**Monitor - sztuk 13**

| | |
|---|---|
| Typ | Monitor komputerowy minimum 23,5”. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| Zastosowanie | Monitor przeznaczony do prac biurowych |

| | |
|---|---|
| Rodzaj ekranu | Płaski |
| Proporcje ekranu | 16:9 |
| Rodzaj panelu | LED, IPS |
| Głośniki | Tak |
| Rozdzielczość | 1920 x 1080 (FullHD) |
| Kąty widzenia | 178°(H)/178°(V) |
| Złącza | 1 x DisplayPort<br>1 x HDMI<br>1xVGA<br>Wejście audio - 1 szt.<br>AC-in (wejście zasilania) - 1 szt.<br>Uwaga: Wymagana ilość nie jest osiągnięta w wyniku stosowania konwerterów, przejściówek, itp. |
| Głośniki | Tak |
| Kabel | Zasilający oraz HDMI |
| Gwarancja | Min. 24 miesiące |
| Pozostałe | Sprzęt ma być fabrycznie nowy tj. nieużywany, nieuszkodzony, nieregenerowany, nieobciążony prawami osób lub podmiotów trzecich i wyprodukowany w okresie 12 miesięcy przed terminem składania ofert oraz pochodzić z legalnego kanału sprzedaży producenta. Wszystkie sztuki laptopów muszą być tego samego rodzaju (ten sam model pochodzący od jednego producenta). |

**Microsoft Office Home & Business 2021: sztuk -15**

- Platforma: Windows
- Okres licencji: Dożywotnia
- Język polski
- wersja fizyczna

Produkt musi być w 100% nowy, wcześniej nie rejestrowany, produkt musi pochodzić z legalnego źródła

**ABBYY FineReader 15 Standard: - Sztuk 2**

- Platforma: Windows
- Okres licencji: Dożywotnia
- Język polski
- wersja fizyczna

Produkt musi być w 100% nowy, wcześniej nie rejestrowany, produkt musi pochodzić z legalnego źródła

Część 2 – Switch, routery WiFi, dyski twarde;

**Switch zarządzalny - sztuk 1**

Wymaga się aby urządzenie jak i zainstalowane zasilacze oraz wentylatory były objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta.
Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii.

Przełącznik powinien obsługiwać następujące standardy oraz protokoły

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z 1000BASE-X
- IEEE 802.3x

Porty:

- 48 x 10/100/1000 Mb/s Ethernet
- 4 x SFP+
- Automatyczne wykrywanie oraz automatyczna negocjacja parametrów połączenia

Wymagane jest aby przełącznik obsługiwał następujące protokoły

- IEEE 802.1D
- IEEE 802.1W
- IEEE 802.1S
- Auto-voice VLAN
- SNMP v1, v2c, v3
- RFC 1213 MIB II
- RFC 1643 Ethernet Interface MIB
- RFC1493 Bridge MIB
- Jumbo Frame
- IEEE 802.1Q Tag VLAN
- 128 Static VLANs
- IEEE 802.1p
- DSCP - L3 QoS
- Ograniczanie pasma na wejściu
- IEEE 802.3ad
- DHCP client
- Broadcast storm control
- Port mirroring (many-to-one)
- Port setting

- IGMP snooping v1/v2
- IEEE 802.1x (RAIDUS)
- ACL - MAC, IP
- SNTP
- IEEE 802.1ab LLDP
- HTTP and HTTPS
- Ochrona przed DoS
- Syslog
- Ping & traceroute
- Konfiguracja przez www
- EEE802.3az
- Statyczny routing
- MLD Snooping

Parametry wydajnościowe

- Metoda przesyłania ramek: Store-and-forward
- Przepustowość magistrali: 100 Gb/s
- Wielkość bufora: 2Mb
- Ilość adresów MAC: 16000
- Czas bezawaryjnej pracy przełącznika 390 tys. godzin

Przełącznik musi spełniać następujące standardy elektromagnetyczne:

- CE mark, commercial
- FCC Part 15 Class A
- VCCI Class A
- EN 55022 (CISPR 22)
- EN 55024 (CISPR 24)
- UL listed (UL 1950)/cUL
- IEC 950/EN 60950
- CE mark, commercial
- CUL 60950 (Listed)/EN 60950 (Low Voltage Directive)

**Router - sztuk 2**

- Technologia sieci WiFi : WiFi 6 (802.11ax)
- 2.4GHz: 600Mbps, 40/20MHz 1024/256-QAM
- 5GHz: 1200Mbps, 80/40/20MHz 1024-QAM

- Liczba portów sieci Ethernet : Pięć portów sieci Gigabit Ethernet 10/100/1000 Mb/s (1 port WAN i 4 porty LAN)
- Procesor min.: Czterordzeniowy procesor 1,5 GHz
- Pamięć min.: 256MB flash and 512MB RAM
- Bezpieczeństwo : Zabezpieczenia WiFi oparte na standardach – 802.11i oraz 128-bitowym szyfrowaniu AES z PSK oraz WPA3
- Obsługa sieci VPN
- Możliwość aktywacji oprogramowania zabezpieczającego domowa sieć przed zagrożeniami pochodzącymi z sieci Internet. Aktywacja usługi daje również prawo do korzystania z oprogramowania antywirusowego na urządzeniach końcowych bezpłatnie.

**Nazwa elementu: Dyski twarde do serwera kopii zapasowych NAS - sztuk 2**

| | |
|---|---|
| **Typ** | Dyski twarde do serwera kopii zapasowych NAS |
| **Zastosowanie** | Monitor przeznaczony do prac biurowych |
| **Pojemność** | 4 TB |
| **Format** | 3.5’’ |
| **Interfejs komunikacyjny:** | SATA III (6.0 Gb/s) |
| **Prędkość obrotowa** | co najmniej 5900 obr./min. |
| **Niezawodność MTBF:** | 1 000 000 godz. |
| **Gwarancja:** | Min. 24 m-ce |

## Część 3 – drukarki do etykiet, czytnik kodów, skaner;

**Drukarka etykiet – sztuk 3**

- Technologia druku: termiczna lub termotransferowy
- Rozdzielczość 203 dpi
- Języki programowania: EPL i ZPL standardowo
- Konstrukcja: podwójne ścianki
- Wymiana głowicy drukującej i wałka bez pomocy narzędzi
- OpenACCESS™ zapewnia łatwe ładowanie nośników
- Automatyczna kalibracja nośników

| | |
|---|---|
| Rodzaj druku: | termiczny |
| Rozdzielczość druku [dpi]: | 203 |
| Maks. prędkość druku [mm/s]: | 127 |

| | |
|---|---|
| Szerokość druku [mm]: | 104 |
| Maks. długość druku [mm]: | 991 |
| Min. szerokość etykiet [mm]: | 19 |
| Szerokość etykiety [mm]: | 108 |
| Min. wysokość etykiet [mm]: | 9.7 |
| Wysokość etykiety [mm]: | 991 |
| Maks. średnica zewn. rolki etykiet [mm]: | 127 |
| Średnica wewn. rolki z etykietami [cale]: | 1 |
| Procesor: | RISC 32 bit |
| Ilość pamięci FLASH: | 004 MB |
| Ilość pamięci RAM: | 008 MB |
| Dostępne interfejsy: | USB, Ethernet |
| Języki programowania: | EPL2, ZPL, ZPL2 |
| Gwarancja producenta [mc]: | Min. 24 |
| Obsługiwane kody kreskowe: | 1D, 2D, GS1 Databar, PDF |

**Czytnik kodów - sztuk 1**

| | |
|---|---|
| TYP SKANERA: | 1D, laser (Standard Range - standardowy zasięg skanowania) |
| Zasięg odczytu: | do 76 cm |
| RODZAJE INTERFEJSU: | USB, RS232, KBW |
| SYGNALIZACJA ODCZYTU: | świetlna, dźwiękowa |
| ODPORNOŚĆ NA UPADKI: | do 1,5 m |
| KABEL W ZESTAWIE: | USB |
| PODSTAWKA W ZESTAWIE: | tak, "gooseneck" |
| Gwarancja PRODUCENTA: | Min 24 miesiące |

**Skaner – sztuk 1**

**Skanowanie**

| | |
|---|---|
| Maksymalny format skanowania | 216 x 5588 mm |
| Optyczna rozdzielczość skanowania | 600 x 600 DPI |
| Podwójne skanowanie | Tak |
| Skanowanie w kolorze | Tak |

| | |
|---|---|
| Głębokość koloru wyjścia | 24 bit |
| Skanowanie kliszy | Nie |
| Prędkość skanowania ADF (cz/b, A4) | 60 stron/min |
| Prędkość skanowania ADF (kolor, A4) | 60 stron/min |
| Prędkość skanowania Flatbed (cz/b, A4) | 1,7 s/str. |
| Prędkość skanowania duplex ADF (cz/b, A4) | 120 ipm |
| Prędkość skanowania duplex ADF (kolor, A4) | 120 ipm |
| Czarnobiałe skanowanie | Skala szarości, Monochromatyczne |

**Konstrukcja**

| | |
|---|---|
| Typ skanera | Skaner płaski/ADF |
| Wbudowany wyświetlacz | Tak |
| Kolor produktu | Czarny, Biały |
| Typ ekranu | LCD |

**Wydajność**

| | |
|---|---|
| Typ przetwornika obrazu | CCD |
| Maksymalny dzienny cykl pracy | 4000 stron(y) |
| Źródło światła | LED |
| Sterowniki skanera | ISIS,TWAIN |

**Pojemność wejściowa**

| | |
|---|---|
| Pojemność automatycznego podajnika papieru | 80 ark. |

**Obsługa papieru**

| | |
|---|---|
| Maksymalny rozmiar papieru ISO (seria A) | A4 |
| Wykrywanie sklejonych stron | Tak |
| Rozmiary seri A ISO (A0…A9) | A4 |
| Gramatura nośników do automatycznego podajnika papieru | 27 - 413 g/m² |
| Maksymalny obszar skanowania (Auto Document Feeder) | 216 x 355,6 mm |
| Minimalny obszar skanowania (Auto Document Feeder) | 50,8 x 54 mm |

**Porty i interfejsy**

| | |
|---|---|
| Port USB | Tak |

**Wymagania systemowe**

| | |
|---|---|
| Obsługiwane systemy operacyjne Windows | Windows 10/11 Pro 64 BIT |

**Gwarancja 24 mies.**

## Część 4 – Laptopy

**Laptop sztuk 1 – poz 1**

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|---|---|
| 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 umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. |
| Ekran | Matryca matowa IPS, 15,6” z podświetleniem w technologii LED, rozdzielczość: FHD 1920x1080. Częstotliwość odświeżania ekranu - 144 Hz. |
| Pamięć operacyjna | Min 32GB z możliwością rozbudowy do 64GB, rodzaj pamięci min. DDR4. |
| Chipset | Dostosowany do zaoferowanego procesora |
| Dysk twardy | Dysk SSD M.2 PCIe<br>512 GB<br>960 GB<br>zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Nie gorsza niż NVIDIA GeForce RTX 3050 Niezintegrowana karta graficzna z pamięcią min. 4GB GDDR6. |
| Porty/złącza | USB 2.0 - 1 szt.<br>USB 3.2 Gen. 1 - 1 szt.<br>USB Typu-C - 1 szt.<br>USB Typu-C (z Thunderbolt™ 4) - 1 szt.<br>HDMI 2.1 - 1 szt.<br>Czytnik kart pamięci microSD - 1 szt.<br>Mini Display Port - 1 szt.<br>RJ-45 (LAN) - 1 szt.<br>Wejście mikrofonowe - 1 szt.<br>Wyjście słuchawkowe/wejście mikrofonowe - 1 szt.<br>DC-in (wejście zasilania) - 1 szt. |
| Klawiatura | Klawiatura z wbudowanym podświetleniem. Wydzielona klawiatura numeryczna |
| Łączność | LAN 1 Gb/s<br>Wi-Fi 6<br>Moduł Bluetooth 5.2 |
| Bateria | Litowo-jonowa |
| Zasilacz | Zasilacz zewnętrzny |

| | |
|---|---|
| BIOS | BIOS zgodny ze specyfikacją UEFI.<br>Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji:<br>- wersji BIOS<br>- nr seryjnym komputera<br>- ilości pamięci RAM<br>- typie procesora i jego prędkości<br>-modele zainstalowanych dysków twardych<br>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:<br>Możliwość ustawienia hasła dla twardego dysku<br>Możliwość ustawienia hasła na starcie komputera tzw. POWER-On PassWord<br>Możliwość ustawienia hasła Administratora i użytkownika BIOS<br>Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU<br>Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,<br>Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. |
| Bezpieczeństwo | - złącze Kensington Lock,<br>- Szyfrowanie TPM |
| Certyfikaty i standardy | Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty)<br>Deklaracja zgodności CE (załączyć do oferty)<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki |
| System operacyjny – w formularzu oferty trzeba podać nazwę oferowanego oprogramowania | Windows 11 Professional 64 bit lub równoważny:<br>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim |

| | |
|---|---|
| | Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>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,<br>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br>Wbudowany system pomocy w języku polskim.<br>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. |
| Gwarancja | Min 2 letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego.<br>- dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) |
| Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.<br>- możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego<br>- Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

**Laptop - sztuk 1 – poz 2**

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|---|---|
| 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 umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. |
| Ekran | Matryca IPS, 15,6” FHD 1920x1080, |
| Jasność matrycy | 300 cd/m² |
| Obudowa | Aluminiowa pokrywa matrycy<br>Aluminiowe wnętrze laptopa<br>Standard militarny MIL-STD-810H |
| Chipset | Dostosowany do zaoferowanego procesora |

| | |
|---|---|
| Wydajność obliczeniowa | Procesor wielordzeniowy zintegrowanym z układem graficznym osiągający w teście wydajności CPU PassMark Performance Test co najmniej wynik 13400 punktów (https://www.cpubenchmark.net) z wynikiem aktualnym nie starszym niż na dzień publikacji ogłoszenia. |
| Pamięć operacyjna | Min 16GB z możliwością rozbudowy do 32GB, rodzaj pamięci min. DDR4, 3200MHz. |
| Dysk twardy | Min. 512GB SSD zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Nie gorsza niż Intel Iris Xe Graphics |
| Dźwięk | Wbudowane głośniki stereo<br>Wbudowany mikrofon |
| Porty/złącza | USB 3.2 Gen. 1 - 2 szt.<br>USB Typu-C (z DisplayPort i Power Delivery) - 1 szt.<br>USB Typu-C (z Thunderbolt™ 4) - 1 szt.<br>HDMI 1.4 - 1 szt.<br>Czytnik kart pamięci SD - 1 szt.<br>RJ-45 (LAN) - 1 szt.<br>Wyjście słuchawkowe/wejście mikrofonowe - 1 szt. |
| Klawiatura | Wydzielona klawiatura numeryczna |
| Łączność | LAN 1 Gb/s<br>Wi-Fi 6<br>Moduł Bluetooth 5.2 |
| Bateria | Litowo-polimerowa, 40 Wh |
| Zasilacz | Tak |
| Bezpieczeństwo | Możliwość zabezpieczenia linką (port Kensington Lock)<br>Szyfrowanie TPM |
| Certyfikaty i standardy | Deklaracja zgodności CE (załączyć do oferty)<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki |
| System operacyjny – w formularzu oferty trzeba podać nazwę oferowanego oprogramowania | Windows 11 Professional 64 bit lub równoważny<br>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych |

| | |
|---|---|
| | Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br><br>Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim<br><br>Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br><br>Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br><br>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,<br><br>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br><br>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br><br>Wbudowany system pomocy w języku polskim.<br><br>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br><br>Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.<br>Klucz produktu przypisany do komputera aby przy ponownej reinstalacji systemu nie było konieczności wpisywania klucza.<br>Możliwość podłączenia do domeny Active Directory. |
| Gwarancja | Min 2-letnia gwarancja świadczona na miejscu u klienta, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi musi oferować przez cały okres :<br>- dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze) |
| Wsparcie techniczne | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.<br>- możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego<br>- Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

## CZĘŚĆ 5 – UTM (URZĄDZENIE, INSTALACJA, KONFIGURACJA, LICENCJA);

**UTM wraz z licencja i wdrożeniem (konfiguracja)**

| | |
|---|---|
| Konstrukcja | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.<br>Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2.<br>Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)<br>Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active.<br>System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.<br>Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne).<br>Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19".<br>Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).<br>Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.<br>Możliwość przeprowadzenia konfiguracji w trybie Zero Touch.<br><br>Pamięć operacyjna RAM nie mniej niż (GB): 6<br>Przestrzeń do przechowywania logów i raportów nie mniej niż (GB) 64<br>Liczba fizycznych interfejsów 1000BASE-T nie mniej niż:12<br>Liczba fizycznych interfejsów 1000BASE-X nie mniej niż: 2<br>Liczba fizycznych interfejsów 10GBASE-X nie mniej niż: 0<br>Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: 256 |
| Wydajność | Wydajność Firewall nie mniej niż (Mbps) 10000<br>Wydajność Firewall IMIX nie mniej niż (Mbps) 4000<br>Wydajność IPS nie mniej niż (Mbps) 25000<br>Wydajność FW+IPS+AV nie mniej niż (Mbps) 800<br>Wydajność NGFW nie mniej niż (Mbps) 2500<br>Liczba równoczesnych połączeń nie mniejsza niż: 5000000<br>Liczba nowych połączeń na sekundę nie mniejsza niż: 60000<br>Wydajność IPsec VPN nie mniej niż (Mbps): 4000<br>Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps): 750<br>Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 1024<br>Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 1000 |

| | |
|---|---|
| | Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: 1000 |
| Zarządzanie | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.<br>Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).<br>Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.<br>Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.<br>Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.<br>Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.<br>System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.<br>System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.<br><br>System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.<br>Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).<br>System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.<br>Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). |

| | |
|---|---|
| | System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).<br>Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.<br>System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).<br>Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.<br><br>System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika).<br>System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.<br>System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta<br>Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji.<br><br>Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. |
| Zapora sieciowa | Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.<br>System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.<br>Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.<br>Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.<br>Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.<br>System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).<br>System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika. |
| Trasowanie ruchu | Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. |

| | |
|---|---|
| | Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.<br>Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.<br>Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.<br>Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).<br>Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).<br>Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6. |
| Translacja adresów i portów | Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT.<br>Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT |
| Kształtowanie pasma i jakość usług | System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.<br>Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.<br>System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.<br><br>Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.<br>Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet. |
| Ochrona przed atakami DoS i DDoS | System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). |
| Pozostałe | Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.<br>Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).<br>System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. |

| | |
|---|---|
| | System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP.<br>Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).<br>System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp.<br>Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).<br>Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).<br>Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych. |
| Uwierzytelnianie i obsługa użytkowników | Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.<br><br>Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.<br>System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.<br>Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.<br>System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).<br><br>Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.<br><br>System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.<br>Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.<br>Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.<br>Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.<br>Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. |

| | |
|---|---|
| | Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. |
| Koncentrator VPN | System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.<br>System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).<br>System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.<br>Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.<br>Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.<br>Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.<br>Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.<br>Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.<br>Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.<br><br>Urządzenie musi obsługiwać połączenia L2TP over IPsec. |
| Logowanie i raportowanie | System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym.<br>System powinien umożliwiać składowanie oraz archiwizację logów.<br>Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.<br>Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa<br>System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.<br><br>System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.<br>Rozwiązanie powinno umożliwiać wysyłanie raportów via email.<br>Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.<br><br>Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. |

| | |
|---|---|
| | System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.<br>System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.<br>Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.<br><br>System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. |
| Intrusion Prevention System i Advanced Threat Protection | Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.<br>Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.<br>Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.<br>Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.<br>System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. |
| Ochrona przez Malware | Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.<br>Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.<br>Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.<br>System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.<br>Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.<br>Rozwiązanie musi przeprowadzać emulację skryptów Java.<br>Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.<br>System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates) |
| Inspecja ruchu SSL/TLS | Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.<br><br>Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.<br>Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.<br>Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). |

| | |
|---|---|
| | Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.<br>Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. |
| Filtr Web | Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron.<br>Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.<br>Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.<br>System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji. |
| Ochrona i kontrola aplikacji | Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji.<br>Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.<br>Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.<br>Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.<br>Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.<br>Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN. |
| Ochrona przed nieznanymi zagrożeniami | Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.<br>Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.<br>Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.<br>Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.<br>Rozwiązanie umożliwiające dodatkową inspekcję i detonację archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.<br>Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików.<br>System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS.<br>System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. |

| | |
|---|---|
| | System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. |
| Ochrona poczty Email | Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Explicit Email Proxy (Mail Transfer Agent).<br>System powinien umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS.<br>Rozwiązanie powinno zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.<br>System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.<br>Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups).<br>Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur zagrożeń.<br>Rozwiązanie powinno zapewniać ochronę przed atakami typu Phishing.<br>System powinien zapewniać wykrywanie, blokowanie i skanowanie załączników.<br><br>Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar.<br>System powinien wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości.<br>Rozwiązanie powinno oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora.<br>System powinien oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP oraz IMAP.<br>Rozwiązanie powinno umożliwiać dodanie stopki do każdej wiadomości wychodzącej.<br>Rozwiązanie powinno umożliwiać konfigurację co najmniej pięciu źródeł RBL (Real-time Blackhole Lists).<br>Rozwiązanie powinno umożliwiać tworzenie globalnych białych i czarnych list adresów IP i email.<br>Rozwiązanie powinno zapewniać wykrywanie spamu niezależnie od stosowanego języka.<br>Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo zarządzać kwarantanną dla wiadomości email.<br>Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo zarządzać swoimi białymi i czarnymi listami adresów email.<br>System powinien oferować mechanizmy weryfikacji odbiorcy wiadomości email (Reciepient verification).<br>Rozwiązanie powinno oferować weryfikację SPF dla wiadomości przychodzących. |

| | |
|---|---|
| | Rozwiązanie powinno umożliwiać uruchomienie funkcji Greylisting.<br>Rozwiązanie powinno umożliwiać filtrowanie załączników na podstawie nagłówków MIME.<br>Rozwiązanie powinno oferować funkcje Bounce Address Tag Validation (BATV).<br><br>Rozwiązanie powinno weryfikować niewłaściwe komunikaty HELO/EHLO i rekordy RDNS.<br>Rozwiązanie powinno weryfikować sygnatury DKIM w nagłówkach wiadomości przychodzących.<br>Rozwiązanie powinno umożliwiać dodawanie sygnatur DKIM do nagłówków wiadomości wychodzących. |
| Konfiguracja | - Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, konfiguracja routingu, DNS, NTP),<br>- Konfiguracja profilów administracyjnych,<br>- Podpięcie weryfikacja statusu licencji,<br>-Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy),<br>- Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa,<br>- Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa,<br>- Konfiguracja lokalnej bazy użytkowników oraz zdefiniowanie grup, oraz podłączenie do usługi<br>- Konfiguracja VPN wg potrzeby<br>- Konfiguracja IPSec VPN site-to-site,<br>- Konfiguracja IPSec VPN client-to-site,<br>- Konfiguracja SSL VPN client -to-site,<br>- Konfiguracja profilów kontroli Antywirusowej i podpięcie do polityk FW,<br>- Konfiguracja profilów ochrony przed atakami IPS i podpięcie do polityk FW<br>- Konfiguracja profilów kontroli aplikacji i podpięcie do polityk FW,<br>- Konfiguracja profilów kontroli WWW i podpięcie do polityk FW,<br>- Konfiguracja profilów antyspamowych i podpięcie do polityk FW,<br>- Test zastosowanych funkcji ochronnych,<br>- Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji. |
| Pozostałe informacje | Wymagane jest 4-dniowe certyfikowane szkolenie dla administratora w wymiarze 32h przez inżynierów certyfikowanych przez producenta dostarczonego rozwiązania klasy UTM |
| Licencja | 36 mies |
| Gwarancja | Min. 24 mies. |