Część I

1. UTM

Obsługa sieci - wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

Firewall - Firewall klasy Stateful Inspection, obsługa translacji adresów NAT n:1, NAT 1:1 oraz PAT. Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów, możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie, możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia, możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.
Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

Intrusion Prevention System (IPS) - System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

Kształtowanie pasma (Traffic Shapping) - Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

Ochrona antywirusowa - rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent

rozwiązania). Licencja na obydwa skanery antywirusowe ma być dostarczana wraz z urządzeniem. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

Ochrona antyspam - producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL, heurystyczny skaner. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

Wirtualne sieci prywatne (VPN) - Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
Odpowiednio kanały VPN można budować w oparciu o: PPTP VPN, IPSec VPN, SSL VPN SSL VPN musi działać w trybach Tunel i Portal. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

Filtr dostępu do stron WWW - Urządzenie ma mieć możliwość wyboru jednego z dwóch filtrów URL: filtra URL wbudowanego na urządzeniu lub filtra URL chmurowego. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. Wbudowany filtr URL ma być stworzony i rozwijany przez polskich inżynierów oraz dedykowany dla polskich użytkowników. Chmurowy filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowy. W ramach chmurowego filtra URL winno być sklasyfikowanych co najmniej 100 milionów stron internetowych. Administrator musi mieć możliwość dodawania własnych kategorii URL. Urządzenie nie może być limitowane pod względem kategorii URL dodawanych przez administratora. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. Administrator winien posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jedna z trzech akcji: blokowanie dostępu do adresu URL, zezwolenie na dostęp do adresu URL, blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. Urządzenie musi posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

Uwierzytelnianie - urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: SSL, Radius, Kerberos.
Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

Administracja łączami do internetu (ISP) - Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: równoważenie względem adresu źródłowego, równoważenie względem połączenia. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.Rozwiązanie powinno wspierać technologię Link Aggregation.

Pozostałe usługi i funkcje rozwiązania - urządzenie ma posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. Urządzenie musi posiadać usługę DNS Proxy.

Administracja urządzeniem - producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
Komunikacja może odbywać się na porcie innym niż https (443 TCP). Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być

zabezpieczona za pomocą protokołu https. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

Raportowanie - urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.

Parametry sprzętowe - urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 320 GB. Liczba portów Ethernet 10/100/1000Mbps – min. 12. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. Przepustowość Firewalla – min. 5 Gbps Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps. Przepustowość filtrowania Antywirusowego – min. 850 Mbps Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500 Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100
Obsługa min. VLAN 256 Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. Urządzenie jest nielimitowane na użytkowników.
Gwarancja min. 36 miesięcy

Część II

1. Punkty dostępowe

Prędkość transferu danych przez Ethernet LAN 10,100,1000 Mbit/s
Maksymalny transfer danych przez bezprzewodowy LAN min. 1300 Mbit/s
Maksymalny zakres wewnętrzny (pomieszczenie) min. 122 m
Ilość portów Ethernet LAN (RJ-45) min. 2
Liczba portów USB 2.0 min. 1
Standard: 802.11 a/b/g/n/ac
Szyfrowanie / bezpieczeństwo min. AES,TKIP,WEP,WPA,WPA2
Możliwość współpracy z serwerem RADIUS
Ilość anten min. 3
Obsługa PoE - Tak, min 802.3at PoE+

Tryb AP - Tak
Tryb WDS z AP - Tak
Tryb AP Client - Tak
Liczba sieci SSID min. 4
Roaming między urządzeniami o wspólnym SID – Tak
Automatyczny wybór optymalnego kanału - Tak
Obsługa VLAN – Tak
Możliwość przypisania SID do VLAN – Tak.
Możliwość stworzenia sieci dla gości z innym typem uwierzytelniania jak podstawowe sieci - Tak

Zestaw do montażu – Tak

Dodatkowo w skład zestawu winny wchodzić:
Zasilacz kompatybilny z urządzeniem dedykowany przez producenta sprzętu dla każdego urządzenia.
Urządzenie musi być kompatybilne z posiadanym kontroler Ubiquiti UniFi UC-CK

Gwarancja min. 12 miesięcy

2. Switch + konwerter światłowodowy

Cechy zarządzania –
- interfejs wiersza poleceń (CLI);
- Przeglądarka internetowa; menu konfiguracyjne;
- zarządzanie pozapasmowe (port szeregowy RS-232C)
- SSH
- Telnet

Wykorzystanie aplikacji internetowej do zarządzania określonymi zadaniami.

Łączność - Podstawowe przełączanie RJ-45
Liczba portów (gniazd) RJ-45 Ethernet. - 24 z automatycznym przełączaniem 10/100/1000
Ilość portów SFP/SFP+ - 4
Ilość slotów Modułu SFP - 4
Port konsoli szeregowej

Sieć komputerowa
Standardy komunikacyjne IEEE 802.1D,IEEE 802.1p,IEEE 802.1Q,IEEE 802.1s,IEEE 802.1w,IEEE 802.3,IEEE 802.3ab,IEEE 802.3af,IEEE 802.3at,IEEE 802.3az,IEEE 802.3u,IEEE 802.3x

System Full-duplex, podpora kontroli przepływu, agregator połączenia, automatyczne MDI/MDI-X MDI, protokół drzewa rozpinającego,

Przepustowość rutowania/przełączania - 56 Gbit/s
Przepustowość - 41600000 Mpps
Maksymalna szybkość przesyłania danych - 1 Gbit/s
Opóźnienie maks 2,3 µs

Protokoły i standardy

Protokoły zarządzające
• RFC 1591
• SSHv1/SSHv2
• RFC 2576
• RFC 2579
• RFC 2580
• RFC 3416
• RFC 3417
Protokoły ogólne
• I EEE 802.1D
• IEEE 802.1p
• IEEE 802.1Q
• IEEE 802.1s
• IEEE 802.1w
• IEEE 802.3
• IEEE 802.3ab
• IEEE 802.3ad
• IEEE 802.3af
• IEEE 802.3at
• IEEE 802.3az
• IEEE 802.3x
• RFC 768 UDP
• RFC 783 TFTP Protocol (revision 2)
• RFC 792 ICMP
• RFC 793 TCP
• RFC 826 ARP
• RFC 854 TELNET
• RFC 868 Time Protocol
• RFC 951 BOOTP
• RFC 1350 TFTP Protocol (revision 2)
• RFC 1542 BOOTP Extensions
• RFC 1918 Address Allocation for Private Internet
• RFC 2030 Simple Network Time Protocol (SNTP) v4
• RFC 2131 DHCP
• RFC 3411
• RFC 3412
• RFC 3413
• RFC 3414
• RFC 3415
• RFC 3575 IANA Considerations for RADIUS
• RFC 5905 NTP Client
• RFC 3376 IGMPv3
Zarządzanie siecią
• IEEE 802.1AB
• RFC 1098 A
• RFC 1155
• RFC 2819
• RFC 3411
• RFC 3412
• RFC 3413

• RFC 3414
• RFC 3415
• RFC 3418
• RFC 5424
• ANSI/TIA-1057 (LLDP-MED)
• SNMPv1/v2c/v3
QoS/CoS
• RFC 2474
• RFC 2475
• RFC 2597
• RFC 2598
Bezpieczeństwo
• IEEE 802.1X Port Based Network Access Control
• RFC 1492 TACACS+
• RFC 2138 RADIUS Authentication
• RFC 2866 RADIUS Accounting
• RFC 7030 Enrollment over Secure Transport
• Secure Sockets Layer (SSL)

Możliwości montowania w stelażu Rack 19”

Taktowanie procesora - 800 Mhz
Pojemność pamięci wewnętrznej - 128 MB
Typ pamięci - DDR3
Wielkość pamięci flash - 128 MB
Pamięci bufora pakietów - 3 MB
Prędkość transferu danych - 10,100,1000 Mbit/s

Dodatkowo do switcha należy dołączyć kompatybilny z urządzeniem konwerter światłowodowy, którego zastosowanie nie spowoduje ograniczenia gwarancji urządzenia. Parametry konwertera:

Min. jeden port LC 1000Base-SX (1000Base-SX typu IEEE 802.3z.

Typ interfejsu - SFP

Maksymalna szybkość przesyłania danych min. 1000 Mbit/s

Złącze światłowodowe - LC

Typ transceivera SFP - SX

Praca

Obsługa funkcji Plug & Play - Tak

Obsługa podłączania podczas pracy - Tak

Automatyczne MDI/MDI-X MDI - Tak

Maksymalny dystans transferu min. 550 m

Typ przewodu - Multi-mode

Moc Tx (minimalna) -9.5 dBm

Moc Tx (maksymalna) -3 dBm

Moc Rx (minimalna) -32 dBm

Gwarancja switch'a oraz konwertera min. 24 miesiące (nie mniej niż gwarancja producenta)

Część III

1. Komputer stacjonarny I

Procesor	Typ procesora osiągający w teście PassMark CPU Mark wynik min. 5700 http://www.cpubenchmark.net/cpu_list.php oraz wynik min. 2215 dla jednego rdzenia https://www.cpubenchmark.net/singleThread.html Wynik testu powinien zostać poświadczony wydrukiem ze strony http://www.cpubenchmark.net/cpu_list.php, wykonanym nie wcześniej niż 2 tygodnie przed upływem terminu składania ofert
Płyta główna	Parametry minimalne: Rodzaj obsługiwanej pamięci - DDR4 Maksymalna wielkość pamięci 64 GB Gniazdo M.2 Tak Liczba gniazd SATA - 6 szt PCIe 3.0 x16 - 1 szt PCI - 2 szt DVI-D - 1 szt HDMI - 1 szt VGA - 1 szt M.2 type 2242/2260/2280/22110 SATA - 1 szt Złącza USB na tylnym panelu: 2 x port USB 2.0/1.1 4 x USB 3.1 Karta dźwiękowa z obsługą 7 kanałów - 1 szt Gigabit LAN
Pamięć	4 GB DDR 4
Dysk twardy	SSD 120 GB 2,5"
Obudowa	2 złącza USB 3.0 w środkowej lub górnej części obudowy umiejscowione na przednim panelu obudowy
Zasilacz	400 W z aktywnym PFC, wentylatorem 12 cm i możliwością podłączenia min. 3 urządzeń SATA
System Operacyjny	Microsoft Windows 10 Pro OEM PL 64 Bit System operacyjny musi być nieużywany i nieaktywowany na jakimkolwiek innym urządzeniu. Wraz z systemem muszą zostać dostarczone wszystkie oryginalne atrybuty legalności określone przez producenta systemu.
Gwarancja	min. 36 miesięcy

2. Komputer stacjonarny II

Procesor	Typ procesora osiągający w teście PassMark CPU Mark wynik min. 5700 http://www.cpubenchmark.net/cpu_list.php oraz wynik min. 2215 dla jednego rdzenia https://www.cpubenchmark.net/singleThread.html Wynik testu powinien zostać poświadczony wydrukiem ze strony http://www.cpubenchmark.net/cpu_list.php, wykonanym nie wcześniej niż 2 tygodnie przed upływem terminu składania ofert
Płyta główna	Parametry minimalne: Rodzaj obsługiwanej pamięci - DDR4 Maksymalna wielkość pamięci 64 GB Gniazdo M.2 Tak Liczba gniazd SATA - 6 szt PCIe 3.0 x16 - 1 szt PCI - 2 szt DVI-D - 1 szt HDMI - 1 szt VGA - 1 szt M.2 type 2242/2260/2280/22110 SATA - 1 szt Złącza USB na tylnym panelu: 2 x port USB 2.0/1.1 4 x USB 3.1 Karta dźwiękowa z obsługą 7 kanałów - 1 szt Gigabit LAN
Pamięć	8 GB DDR 4
Dysk twardy I	SSD 120 GB 2,5”
Dysk twardy II	4TB sATA III 64MB
Obudowa	2 złącza USB 3.0 w środkowej lub górnej części obudowy umiejscowione na przednim panelu obudowy
Zasilacz	400 W z aktywnym PFC, wentylatorem 12 cm i możliwością podłączenia min. 3 urządzeń SATA
System Operacyjny	Microsoft Windows 10 Pro OEM PL 64 Bit System operacyjny musi być nieużywany i nieaktywowany na jakimkolwiek innym urządzeniu. Wraz z systemem muszą zostać dostarczone wszystkie oryginalne atrybuty legalności określone przez producenta systemu.
Gwarancja	min. 36 miesięcy

3. Licencja Windows Server

Windows Server Standard Core 2016 Sngl OLP 16Licenses NoLevel CoreLic PL
Zastosowana licencja nie może ograniczać maksymalnej ilości użytkowników.

Zamawiający nie jest uprawniony do korzystania z wersji oprogramowania GOV ani EDU

Część IV

1. Laptop + Torba

Procesor	Typ procesora osiągający w teście PassMark CPU Mark wynik min. 7600 http://www.cpubenchmark.net/cpu_list.php oraz wynik min. 1900 dla jednego rdzenia https://www.cpubenchmark.net/singleThread.html Wynik testu powinien zostać poświadczony wydrukiem ze strony http://www.cpubenchmark.net/cpu_list.php, wykonanym nie wcześniej niż 2 tygodnie przed upływem terminu składania ofert
Ekran	Wyświetlacz od 15 do 16 cali (1920 x 1080 (Full HD)) powłoka matrycy Matowa
Karta graficzna	pamięć własna karty graficznej min.2 GB
Pamięć	min. 8 GB DDR4 z możliwością rozbudowy do min. 16 GB
Napęd optyczny	napęd DVDRW
Dysk twardy	wbudowany dysk SSD min. 256 GB M.2 + wbudowany dysk HDD min. 1 TB
Dźwięk	Wbudowane dwa głośniki, Wbudowany mikrofon
Klawiatura	Układ QWERTY z wydzieloną częścią numeryczną
Urządzenie wskazujące	TouchPad
Kamera	Wbudowana kamera
Karta sieciowa	10/100/1000 (RJ-45)
Łączność bezprzewodowa	Bluetooth 4.1, WiFi 802.11 ac
Porty USB	Ilość portów USB min. 2xUSB 3.0 i min. 1x USB typ C
Gniazda rozszerzeń	Czytnik kart pamięci
Złącza	HDMI, Wyjście słuchawkowe/wejście mikrofonowe
Opcje dodatkowe	możliwość zabezpieczenia linką (port typu Kensington Lock), sprzętowe wsparcie szyfrowania AES, czytnik linii papilarnych, TPM
Zasilacz	w zestawie
Torba	Torba min. 2 komory, usztywniana, uchwyt oraz pasek na ramię, kolor dominujący – czarny, rozmiar dedykowany do zaproponowanego laptopa
System Operacyjny	Windows 10 PL Pro lub wyższy, System operacyjny musi być nieużywany i nieaktywowany na jakimkolwiek innym urządzeniu. Wraz z systemem muszą zostać dostarczone wszystkie oryginalne atrybuty legalności określone przez producenta systemu.
Gwarancja	24 miesiące