Znak sprawy:

Załącznik nr 1 do Umowy …….
z dnia ……

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa sprzętu komputerowego na potrzeby Zarządu Transportu Miejskiego w Poznaniu.

Kody CPV:
30213100-6 – „Komputery przenośne"
30237200-1 – „Akcesoria komputerowe"
32420000-3 – „Urządzenia sieciowe"

1. Informacje ogólne dotyczące przedmiotu zamówienia:

Przedmiot zamówienia został podzielony na 4 Części (tj. zadania), których zakres przedmiotowy opisano poniżej. Zamawiający dopuszcza możliwość składania ofert częściowych, Wykonawca może złożyć tylko jedną ofertę na dowolną liczbę Części. Zamawiający nie wyraża zgody na złożenie oferty obejmującej jedynie wybrane pozycje w ramach jednej Części.

Część 1 – uniwersalny laptop

Lp.	Opis	Ilość
1.	Laptop zwykłego przeznaczenia	27 sztuk
2.	Stacja dokująca do laptopa z pkt. 1	21 sztuk

Część 2 – laptop ultra-mobilny

Lp.	Opis	Ilość
1.	Laptop ultramobilny	1 sztuk

Część 3 – akcesoria komputerowe

Lp.	Opis	Ilość
1.	Klawiatura przewodowa	27 sztuk
2.	Myszka komputerowa	26 sztuk
3.	Bezprzewodowa myszka komputerowa	5 sztuk
4.	Stereofoniczny zestaw słuchawkowy	27 sztuk
5.	Adapter USB-C - mini jack dedykowana do tabletu Samsung SM-T865	4 sztuki

Część 4 – sprzęt zabezpieczenia sieci

Lp.	Opis	Ilość
1.	Zapora ogniowa	1 zestaw

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 1:

1. Wymagania technologiczne i funkcjonalne dla oferowanego laptopa zwykłego przeznaczenia lub równoważny produkt

Komputer przenośny firmy Dell, model Latitude 5520, zgodny z numerem producenta **S002L552015PL**, który jest startowym (bazowym) modelem z podstawowymi parametrami technicznymi. Zamawiający wymaga dostawy ww. notebooka o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Znak sprawy: Załącznik nr 1 do Umowy .....
z dnia .....

Lp.	Opis	Minimalne wymagania techniczne
1.	**Sprzęt zgodny z poniższą specyfikacją:**	
2.	Procesor	Zainstalowany procesor, 4-rdzeniowy w architekturze x86 zaprojektowany do pracy w komputerach przenośnych taktowany zegarem co najmniej dla jednego rdzenia 4.20GHz w trybie Turbo. Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik min.: 10087 punktów (wynik zaproponowanego procesora musi znajdować się na stronie https://www.cpubenchmark.net/laptop.html). Procesor musi posiadać minimum 8 MB pamięci cache oraz wspierać pamięci typu DDR4-3200, LPDDR4x-4267.
3.	Płyta główna	Płyta główna z chipsetem rekomendowanym przez producenta procesora.
4.	Pamięć RAM	Jeden moduł pamięci o pojemności 8 GB (DDR4, 3200MHz) z możliwością rozbudowy do 64 GB. Wyposażony w 2 gniazda pamięci. Zajęte jest jedno gniazdo.
5.	Nośnik danych	Dysk SSD M.2 NVMe PCIe o pojemności 256 GB.
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: Dysk SSD M.2 NVMe PCIe o pojemności 512 GB.
6.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Zaproponowana karta musi mieć w teście PassMark - G3D Mark wynik wydajności na poziomie minimum: 2865 punktów. Wynik zaproponowanej karty musi się znajdować na stronie: https://www.videocardbenchmark.net/high_end_gpus.html.
7.	Ekran	Matryca 15,6" LED w technologii WVA lub IPS, rozdzielczość co najmniej: 1920 x 1080 (FullHD). Powłoka antyodblaskowa, matowa przeciwodblaskowa, z podświetleniem WLED.
8.	Dźwięk	Wbudowane głośniki stereo oraz wbudowane dwa mikrofony.
9.	Klawiatura	Podświetlana w kolorze białym, Typu QWERTY w tzw. układzie amerykańskim (klawisz ze znakiem dolara, a nie funta angielskiego), konieczne występowanie dwóch klawiszy ALT. Wydzielona klawiatura numeryczna. Klawiatura odporna na zalanie.

10.	Wbudowane w sposób trwały interfejsy zewnętrzne	• gniazdo uniwersalne audio
		• HDMI lub DisplayPort lub Mini DisplayPort z dołączoną przejściówką na HDMI umożliwiającą przesyłanie obrazu i dźwięku w jakości HD
		• RJ45 wbudowane o przepustowości 1000 Mb/s
		• co najmniej 4 porty USB, w tym:
		  ○ co najmniej 1 port USB 3.2 Gen. 1,
		  ○ co najmniej 1 port USB 3.2 Gen. 1 (z PowerShare),
		  ○ co najmniej 2 porty USB Typu-C (z Thunderbolt™ 4),
		• czytnik kart pamięci microSD
		• kamera internetowa na podczerwień
		• czytnik Smart Card.

11.	Sieć	• LAN 1Gb/s, zintegrowany z płytą główną; • WiFi 6, standardy sieciowe Wi-Fi 4 (802.11 a/b/g/n), Wi-Fi 5 (802.11 a/b/g/n/ac), Wi-Fi 6 (802.11 a/b/g/n/ac/ax); • Moduł Bluetooth.

12.	Zabezpieczenia	• Układ pozwalający na szyfrowanie danych dysku twardego, TPM 2.0 (klucze szyfrujące, przechowywane w dedykowanym układzie scalonym zintegrowanym z płytą główną, zamiast na dysku twardym) współpracujący z oprogramowaniem dostarczonym wraz z komputerem, wraz z licencją aktywującą (jeśli jest wymagana) • Możliwość zabezpieczenia linką, • Kamera internetowa z wbudowaną zaślepką.
13.	Panel dotykowy	Touchpad, umieszczony pod klawiaturą.
14.	Akumulator	co najmniej 63 Wh.
15.	System operacyjny	Microsoft Windows 10 Pro PL (wersja 64-bitowa), Licencja na system operacyjny Microsoft Windows 10 Pro x64 PL lub równoważny. Klucz instalacyjny systemu operacyjnego powinien być fabrycznie zapisany w BIOS komputera i wykorzystywany do instalacji tego systemu oraz jego aktywowania. System operacyjny ma być fabrycznie zainstalowany przez producenta. Możliwość aktualizacji do Windows 11 odpowiedniej wersji jak 10 Pro PL.
16.	Zasilanie zewnętrzne	Zewnętrzny zasilacz sieciowy AC/DC 100/230V, 60/50Hz, z kablami połączeniowymi
17.	Waga	Do 1,60 kg.
18.	Torba	Dostosowana do rozmiaru oferowanego komputera przenośnego. Torba musi być opcją producenta.
19.	Gwarancja i serwis	Minimum 36 miesięcy gwarancji oraz serwisu, zapewniając naprawę lub dostawę podzespołu zapasowego na następny dzień roboczy. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7. W całym okresie gwarancji uszkodzone dyski pozostają własnością Zamawiającego.

2. Wymagania technologiczne i funkcjonalne dla oferowanej stacji dokującej przeznaczonej dla laptopa z pkt. 1 lub równoważny produkt

Stacja dokująca firmy Dell, model DOCK WD19S 130W USB-C , zgodny z numerem producenta **210-AZBX**, który jest startowym (bazowym) modelem z podstawowymi parametrami technicznymi. Zamawiający wymaga dostawy ww. stacji dokującej o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	Typ	Replikator portów
2.	Interfejs	USB-C
3.	Rodzaje wejść/wyjść	co najmniej USB 3.0 - 3 szt. co najmniej USB 3.0 Typ C - 1 szt. co najmniej USB Typu-C (z DisplayPort) - 1 szt. co najmniej HDMI - 1 szt. RJ-45 (LAN) - 1 szt. co najmniej DisplayPort - 2 szt. DC-in (wejście zasilania) - 1 szt.
4.	Zasilanie	Sieciowe

5.	Dodatkowe informacje	Plug & Play Możliwość zabezpieczenia linką (Kensington Lock) Funkcja Power Delivery
6.	Waga	Minimum 590g
7.	W zestawie	Dołączony zasilacz sieciowy wraz z kablami połączeniowymi.
8.	Gwarancja	12 miesięczna gwarancja producenta.
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: 24 miesięczna gwarancja producenta.

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 2:

1. Wymagania technologiczne i funkcjonalne dla laptopa ultramobilnego lub równoważny produkt

Komputer przenośny firmy ASUS, model ZenBook Flip S, zgodny z numerem producenta **UX371EA-HL003R**, który jest startowym (bazowym) modelem z podstawowymi parametrami technicznymi. Zamawiający wymaga dostawy ww. notebooka o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	**Sprzęt zgodny z poniższą specyfikacją:**	
2.	Procesor	Zainstalowany procesor, 4-rdzeniowy w architekturze x86, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej dla jednego rdzenia 4.70GHz w trybie Turbo. Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik min.: 10648 punktów (wynik zaproponowanego procesora musi znajdować się na stronie https://www.cpubenchmark.net/laptop.html). Procesor musi posiadać minimum 12 MB pamięci cache oraz wspierać pamięci typu DDR4-3200 oraz LPDDR4x-4267.
3.	Płyta główna	Płyta główna z chipsetem rekomendowanym przez producenta procesora.
4.	Pamięć RAM	Minimum 16 GB (LPDDR4x, 4266MHz).
5.	Nośnik danych	Dysk SSD M.2 NVMe PCIe o pojemności 512 GB.
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: Dysk SSD M.2 NVMe PCIe o pojemności 1 TB.
6.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Zaproponowana karta musi mieć w teście PassMark - G3D Mark. Wynik wydajności na poziomie minimum: 2865 punktów (wynik zaproponowanej karty musi się znajdować na stronie https://www.videocardbenchmark.net/high_end_gpus.html.
7.	Ekran	Matryca 13,3” w technologii OLED, rozdzielczość co najmniej: 3840 x 2160 (4K).
8.	Dźwięk	Wbudowane głośniki stereo oraz wbudowane dwa mikrofony.

9.	Klawiatura	Podświetlana w kolorze białym, Typu QWERTY w tzw. układzie amerykańskim (klawisz ze znakiem dolara, a nie funta angielskiego), konieczne występowanie dwóch klawiszy ALT.
10.	Wbudowane w sposób trwały interfejsy zewnętrzne	• USB 3.2 Gen. 1 - 1 szt. • USB Typu-C (z Thunderbolt™ 4) minimum 2 szt. z obsługą sygnału wideo / dostarczania zasilania. • HDMI - 1 szt.
11.	Sieć	• LAN 1Gb/s, zintegrowany z płytą główną albo dołączany poprzez port USB; • Wi-Fi 6; • moduł Bluetooth.
12.	Zabezpieczenia	• Układ pozwalający na szyfrowanie danych dysku twardego, TPM 2.0 (klucze szyfrujące, przechowywane w dedykowanym układzie scalonym zintegrowanym z płytą główną, zamiast na dysku twardym) współpracujący z oprogramowaniem dostarczonym wraz z komputerem, wraz z licencją aktywującą (jeśli jest wymagana) • Kamera na podczerwień (IR) z obsługą Windows Hello
13.	Kamera Internetowa	Kamera HD z technologią podczerwieni do obsługi funkcji Windows Hello.
14.	Panel dotykowy	Touchpad, umieszczony pod klawiaturą.
15.	Obudowa	Aluminiowa pokrywa matrycy Aluminiowe wnętrze laptopa Aluminiowa obudowa Klasa MIL-STD 810G
16.	Akumulator	co najmniej 67 WHr
17.	System operacyjny	Microsoft Windows 10 Pro PL (wersja 64-bitowa), Licencja na system operacyjny Microsoft Windows 10 Pro x64 PL lub równoważny. Klucz instalacyjny systemu operacyjnego powinien być fabrycznie zapisany w BIOS komputera i wykorzystywany do instalacji tego systemu oraz jego aktywowania. System operacyjny ma być fabrycznie zainstalowany przez producenta. Możliwość aktualizacji do Windows 11 odpowiedniej wersji jak 10 Pro PL.
18.	Zasilanie zewnętrzne	Zewnętrzny zasilacz sieciowy AC/DC 100/230V, 60/50Hz, z kablami połączeniowymi.
19.	Waga	Do 1,25 kg.
20.	Torba	Dostosowana do rozmiaru oferowanego komputera przenośnego. Torba musi być opcją producenta.
21.	Wyposażenie dodatkowe	Jeśli konieczne, to: Adapter USB dla LAN Adapter USB na audio mini-jack Rysik do obsługi ekranu Firmowe etui na laptopa
22.	Gwarancja i serwis	Minimum 24 miesięcy gwarancji oraz serwisu, zapewniając naprawę lub dostawę podzespołu zapasowego na następny dzień roboczy. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7. W całym okresie gwarancji uszkodzone dyski pozostają własnością Zamawiającego.

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 3:

1. Wymagania technologiczne i funkcjonalne dla oferowanej klawiatury przewodowej lub równoważny produkt

Klawiatura firmy Logitech model: K120, kod producenta: **920-002509** o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	Typ	Nisko profilowa, klasyczna
2.	Układ klawiszy	Typu QWERTY w tzw. układzie amerykańskim (klawisz ze znakiem dolara, a nie funta angielskiego), konieczne występowanie dwóch klawiszy ALT. Osobny panel klawiszy numerycznych
3.	Rodzaj przełączników	Membranowe
4.	Łączność	Przewodowa
5.	Interfejs	USB
6.	Zgodność z systemem	System operacyjny Windows 10/11
7.	Długość przewodu	1,5 m
8.	Dodatkowe informacje	Regulowane stopki Stopki antypoślizgowe Odporność na zachlapanie
9.	Waga	Minimum 550 g.
10.	Gwarancja	24 miesiące
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: 36 miesięcy

2. Wymagania technologiczne i funkcjonalne dla oferowanej myszki przewodowej lub równoważny produkt

Myszka przewodowa firmy Logitech model: M90, kod producenta: **910-001794 / 910-001793** o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	Łączność	Przewodowa
2.	Sensor	Optyczny
3.	Liczba przycisków	3
4.	Rolka przewijania	1
5.	Interfejs	USB
6.	Rozdzielczość	1000dpi
7.	Profil	Praworęczny

8.	Waga	Minimum 90g
9.	Gwarancja	24 miesięcy
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: 36 miesięcy

3. Wymagania technologiczne i funkcjonalne dla oferowanej myszki bezprzewodowej lub równoważny produkt

Myszka bezprzewodowa firmy Logitech model: MX Anywhere 2S, kod producenta: **910-005153** o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	Łączność	Bezprzewodowa
2.	Sensor	Laserowy
3.	Liczba przycisków	7
4.	Rolka przewijania	1
5.	Interfejs	2,4GHz Bluetooth
6.	Odbiornik	W technologii Unifying lub równoważnej, pozwalająca na jednym odbiorniku połączyć do 6 urządzeń. Zasięg minimum 10m. Odbiornik w zestawie.
7.	Zasilanie	Wbudowany akumulator, kabel USB do zasilania w komplecie
8.	Rozdzielczość	4000dpi
9.	Czas pracy na baterii	Do 2 miesięcy
10.	Profil	Praworęczny
11.	Waga	Minimum 106g
12.	Gwarancja	24 miesiące
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: 36 miesięcy

4. Wymagania technologiczne i funkcjonalne dla Stereofonicznego zestawu słuchawkowego USB lub produkt równoważny

Stereofoniczny zestaw słuchawkowy firmy Sennheiser model: PC 5 CHAT, kod producenta: **508328** o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	Złącze	3,5 mm minijack
2.	Budowa słuchawek	Nauszne otwarte
3.	Pasmo przenoszenia słuchawek	42 ~ 17000 Hz

4.	Impedancja słuchawek	32 Ω
5.	Czułość słuchawek	95 dB
6.	Typ głośnika	Neodymowe
7.	Wbudowany mikrofon,	Pasmo przenoszenia mikrofonu: 90 ~ 15000 Hz,
8.	Długość kabla	2,0m
9.	Waga	Minimum 77g
10.	Gwarancja	24 miesiące
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: 36 miesięcy

5. Wymagania technologiczne i funkcjonalne dla Adapter USB-C - mini jack dedykowana do tabletu Samsung SM-T865 lub produkt równoważny

Adapter USB-C - mini jack firmy Samsung, kod producenta: **EE-UC10JUWEGWW** o poniższych parametrach (konfiguracji i opcjach), które są jednocześnie minimalnymi warunkami równoważności:

Lp.	Opis	Minimalne wymagania techniczne
1.	Interfejs	24bit / 192kHz 100dB SNR, wykrycie słuchawek, wykrycie oporności
2.	Adapter	USB Typ C - Jack 3,5mm
3.	Kompatybilność	Galaxy Tab S6 (SM-T865)
4.	Waga	Minimum 3,1 grama
5.	Gwarancja	24 miesiące
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: 36 miesięcy

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 4:

1. Wymagania technologiczne i funkcjonalne dla oferowanej zapory ogniowej Fortinet lub równoważny

Zapora ogniowa firmy Fortinet, model FG-200E zgodny z numerem producenta **FG-200E-BDL-950-36** lub równoważny produkt spełniający poniższe warunki (dalej jako system):

Lp.	Opis	Minimalne wymagania techniczne
1.	Wymagania ogólnie	Dostarczony system musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu 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, • monitorowania na porcie SPAN. W ramach dostarczonego systemu musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: • rutingu, • firewalla, • IPSec VPN, • antywirus, • IPS, • kontroli aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • firewall, • ochrony w warstwie aplikacji, • protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	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. System musi umożliwiać zbudowanie systemu w postaci redundantnej. Monitoring oraz wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:** Zamawiający posiada firewall Fortinet FG-200E, dostarczony system musi pozwalać na zestawienie w klaster Active-Active oraz włączenie synchronizacji sesji firewall.
3.	Interfejsy i zasilanie	System musi dysponować minimum: • 18 portami Gigabit Ethernet RJ-45. • 4 gniazdami SFP 1 Gbps. System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi być wyposażony w zasilanie AC zgodnie ze standardem używanym w Polsce.
4.	Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.

		Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 7.2 Gbps. 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 2.2 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 820 Mbps.
5.	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: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • 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. • Analiza ruchu szyfrowanego protokołem SSL. • Analiza ruchu szyfrowanego protokołem SSH.
6.	Polityki firewall	Polityka firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 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. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
7.	Połączenia VPN	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. 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.
8.	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
9.	Zarządzanie pasmem	System musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
10.	Kontrola antywirusowa	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
11.	Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
12.	Kontrola aplikacji	Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza kontroli aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

		Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności na przykład wysyłanie czy pobieranie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
13.	Kontrola stron WWW	Moduł kontroli stron WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 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. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
14.	Uwierzytelnianie użytkowników w ramach sesji	System 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
15.	Zarządzanie	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. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16.	Logowanie	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.

		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. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
17.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall. • ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW. • ICSA dla funkcji IPSec VPN. • ICSA dla funkcji SSL VPN.
18.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować na okres 36 miesięcy: • kontrola aplikacji, • IPS, • antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), • analiza typu Sandbox, • antyspam, • filtrowanie stron WWW (web filtering), • bazy reputacyjne adresów IP/domen.
19.	Wymagania dodatkowe	Zamawiający wymaga, iż powyższy system będzie współpracował z posiadanym przez Zamawiającego zaporą ogniową Fortinet FG-200E.
20.	Warunki gwarancji	System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie zgłoszonych usterek i awarii lub wymianie urządzenia w przypadku jego wadliwości, która uniemożliwia naprawę. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania. Wsparcie techniczne w trybie 8x5 (8 godzin x 5 dni w tygodniu).

2. Wymagania Zamawiającego dotyczące przedmiotu zamówienia:

Zamawiający wymaga, aby dostarczony sprzęt był fabrycznie nowy, w oryginalnych, nieotwieranych opakowaniach oraz musi pochodzić z oficjalnej dystrybucji na terytorium Rzeczpospolitej Polski. Zamawiający nie dopuszcza dostarczenia produktów w nieoryginalnych opakowaniach, produktów tzw. „refurbished", produktów nieposiadających ważnej gwarancji bez możliwości weryfikacji na stronie producenta produktu.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca 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.

Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Wykonawca przekaże Zamawiającemu spis dostarczanego sprzętu wraz z numerami seryjnymi w formie papierowej i elektronicznej. Każdy z zamawianych elementów musi posiadać swój unikalny numer seryjny.