Opis Przedmiotu Zamówienia

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

1. Informacje ogólne dotyczące przedmiotu zamówienia:

Przedmiot zamówienia został podzielony na 3 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 – sprzęt serwerowy

Lp.	Opis	Ilość
1.	Macierz dyskowa	1 zestaw

Część 2 – sprzęt dyskowy

Lp.	Opis	Ilość
1.	Jednostka dyskowa z nośnikami i z kartą rozszerzeń	1 zestaw

Część 3 – sprzęt zabezpieczenia sieci

Lp.	Opis	Ilość
1.	Zapora ogniowa	1 zestaw

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 1: Wymagania technologiczne i funkcjonalne dla oferowanej macierzy dyskowej

Lp.	Opis	Minimalne wymagania techniczne
1.	**System zgodny z poniższą specyfikacją:**	
2.	Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''.
3.	Pojemność	System musi zostać dostarczony w konfiguracji zawierającej minimum 8 dysków 1,92 TB typu SSD NVMe. System musi posiadać możliwość rozbudowy o kolejne dyski i wspierać dedykowane dyski typu SSD NVMe w zakresie pojemności od 1,92 TB do 15,3 TB. Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania lub migracji danych. Zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz wydajniejszymi procesorami. System musi mieć możliwość rozbudowy do 48 dysków SSD NVMe.

4.	Kontroler	Zainstalowane dwa kontrolery wyposażone w przynajmniej 128 GB pamięci RAM (sumarycznie dla dwóch kontrolerów). Kontrolery te muszą pracować w trybie wysokiej dostępności. Zamawiający wymaga aby dostarczone kontrolery posiadały procesory wykonane w architekturze Intel lub AMD. Dopuszczalne jest zastosowanie procesorów w innej architekturze, przy zachowaniu minimalnej ilości 64 rdzeni na procesor. W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną. Macierz musi pozwalać na rozbudowę do klastra 24 kontrolerów lub musi pozwalać na obsługę przynajmniej 1500 dysków w obrębie pary kontrolerów lub klastra w zależności od sposobu realizacji funkcjonalności. Dodatkowo wymagane jest aby była możliwa rozbudowa o minimum 576 nośników SSD NVMe w ramach klastra lub pary kontrolerów. Wszystkie kontrolery muszą pracować pod kontrolą tego samego systemu operacyjnego stworzonego przez producenta urządzenia. Nie dopuszcza się zastosowania systemu, w którym udostępnianiem danych zarządzają różne systemy operacyjne w jednym zintegrowanym urządzeniu.
5.	Interfejsy	Oferowany system musi posiadać minimum: • 4 porty 25GbE, • 4 porty 10GbE Base-T (RJ45), • 8 portów 32Gb FC.
6.	System RAID	System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID.
7.	Kopie migawkowe	Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/- 5 %.
8.	Obsługiwane protokoły	Macierz musi obsługiwać jednocześnie protokoły FC, FCoE, FC/NVMe, iSCSi, CIFS (SMB) i NFS oraz udostępnianie danych protokołem S3. Jeśli wymagane są licencje Zamawiający wymaga dostarczenia ich wraz z macierzą.
9.	Funkcjonalności	System musi mieć możliwość połączenia w klaster z posiadaną przez Zamawiającego macierzą NetApp FAS2750 w celu migracji wolumenów bez przerwania dostępu do danych. Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych in-line. Macierz musi oferować funkcjonalność kompresji typu inline (dane w znajdujące się w pamięci cache przed zapisaniem na dyski) oraz postprocess (dane umiejscowione na dyskach) dla wszystkich rodzajów udostępnianych danych. Jeżeli oferowane rozwiązanie nie pozwala na deduplikację i kompresję w locie lub nie posiada możliwości deduplikacji i kompresji

		zamawiający wymaga dostarczenie czterokrotnej pojemności wyspecyfikowanej w punkcie 3 niniejszej tabeli. Macierz musi posiadać wsparcie dla wielu ścieżek dla systemów Windows, Linux, VMware, Unix. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność priorytetyzacji zadań. Macierz musi pozwalać funkcjonalność replikacji danych z inną macierzą tego samego producenta w trybie synchronicznym oraz asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikacji replikowanych danych. Macierz musi być dostarczona z sprzętem i/lub odpowiednią licencją, aby umożliwić szyfrowanie wybranego wolumenu, szyfrowanie może się odbywać poprzez zewnętrzne narzędzie szyfrujące lub może być realizowane mechanizmem macierzy. Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. Z macierzą Zamawiający wymaga dostarczenia oprogramowania, które pozwala na: • monitoring wykorzystania przestrzeni na macierzy, • monitoring grup RAID, • monitoring wykonywanych backupów/replikacji danych między macierzami, • monitoring wydajności macierzy, • analizę i diagnozę spadku wydajności. Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną maksymalną pojemność macierzy. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności: • Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego. o procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.

		○ procedura musi uwzględniać systemy zależne np. macierze replikujące. ○ procedura musi umożliwiać generowanie planu cofnięcia aktualizacji. • Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom macierzy. • Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji. • System automatycznego i proaktywnego wsparcia dla macierzy z użyciem sztucznej inteligencji. Portal lub oprogramowanie może pochodzić od innego producenta niż producent macierzy pod warunkiem, iż zostanie dostarczona odpowiednia licencja do maksymalnej pojemności macierzy. **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:** Zamawiający posiada macierze NetApp FAS8200, FAS8020 oraz FAS2750, dostarczony system musi pozwalać na zestawienie replikacji macierzowej poprzez natywny mechanizm z posiadanymi ww. systemami.
10.	Wymagania dodatkowe	Zamawiający wymaga, iż powyższy system będzie współpracował z posiadanymi przez Zamawiającego dwoma przełącznikami SAN Dell DS-6610B. W zestawie niezbędne okablowane (m.in. patchcordy FC) oraz zainstalowane w każdym kontrolerze cztery moduły (wkładki) 32 Gb FC MM SFP+ umożliwiające komunikację z modułami (wkładkami) zainstalowanymi w ww. przełącznikach SAN.
11.	Gwarancja i serwis	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 przypadku awarii krytycznej, serwis zapewni odpowiedź na zgłoszenie do 2 godzin od zgłoszenia. Serwis urządzeń musi być realizowany zgodnie z zaleceniami gwarancyjnymi producenta. Serwis nie może spowodować unieważnienia gwarancji. Serwis musi być wykonywany w miejscu instalacji sprzętu. Dostarczony system musi posiadać również 36 miesięcy subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. System musi pochodzić z autoryzowanego kanału dystrybucji producenta i być objęta serwisem producenta na terenie Polski oraz nie będzie wersją OEM. W całym okresie gwarancji uszkodzone dyski pozostają własnością Zamawiającego.

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 2:

Wymagania technologiczne i funkcjonalne dla oferowanej jednostki dyskowej z nośnikami i z kartą rozszerzeń

Typ i kompatybilność	**Dedykowana jednostka rozszerzająca serwer plików w posiadaniu Zamawiającego: Synology RS18017xs+**

Rodzaj obudowy i elementy montażu	Obudowa o wysokości maksymalnie 2U, przystosowana do zamontowania w szafie rack 19”. Dostarczona jednostka dyskowa musi posiadać wszelkie elementy do montażu. Do zestawu muszą być dołączone dedykowane szyny do mocowania w szafie rack pozwalające na wysuwanie urządzenia do celów serwisowych oraz niezbędne okablowanie (zasilanie oraz kabel rozszerzenia typu Mini-SAS HD).
Wnęki na dyski twarde	Możliwość instalacji minimum 12 dysków twardych wielkości 3,5 cala (lub 2,5 cala z użyciem dedykowanych kieszeni dyskowych). Jednostka musi zawierać pełną klatkę na dyski twarde na przód obudowy wraz z niezbędnymi elementami pozwalającymi na obsługę wszystkich dysków twardych.
Porty zewnętrzne	Z tyłu obudowy muszą się znaleźć porty: • Minimum 1 porty SAS typu wejściowego (IN), • Minimum 1 porty SAS typu wyjściowego (OUT). Dedykowany wskaźnik identyfikacyjny jednostki rozszerzającej.
Zasilanie serwera	Dostarczona jednostka musi posiadać dwa zasilacze w trybie pełnej redundancji z możliwością wymiany zasilacza na gorąco.
System wentylacji	Wymiana na gorąco podczas pracy serwera, bez użycia narzędzi.
Wentylatory	Minimum 4 zainstalowane wentylatory.
Zainstalowane nośniki w jednostce dyskowej zgodne z poniższą specyfikacją:	
Sumaryczna ilość dysków	8 dysków twardych wielkości 3,5 cala klasy enterprise. Wszystkie dyski muszą być obsługiwane przez jednostkę dyskową i współdziałającej z serwerem plików, zgodnie z wytycznymi firmy Synology: https://www.synology.com/pl-pl/compatibility.
Stan	Fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia. Muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
Rodzaj nośnika	Magnetyczny.
Pojemność	Minimum 14 TB dla każdego zainstalowanego nośnika. **FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT:** Co najmniej 16 TB dla każdego zainstalowanego nośnika.
Wbudowana pamięć podręczna	512 MB.
Wydajność	Minimum 255 MB/s.
Interfejs	SATA 6G (trzeciej generacji).
Typ	Możliwość wkładania i wyciągania dysku na gorąco w trakcie pracy.
Prędkość obrotowa talerzy	Co najmniej 7,2 tysiące obrotów na minutę.
Cykle ładowania/ rozładowania	Minimum 580 000 cykli.
Nominalny czas pracy	Minimum 2 500 000 godzin.
Dodatkowe warunki spełniające dla zestawu (jednostki z nośnikami) jak poniżej:	
Pochodzenie	Zestaw jednostki z nośnikami musi być fabrycznie nowy i zamknięty. Nieużywany wcześniej w żadnych projektach, wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia. Musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
Dołączony do zestawu karta rozszerzeń M.2 SSD z nośnikami	

Typ i kompatybilność	**Dedykowana karta współpracująca z serwerem plików w posiadaniu Zamawiającego: Synology RS18017xs+**
Interfejs magistrali hosta	PCIe 2.0 x8.
Profil karty	Nisko i pełnej wysokości.
Interfejs pamięci masowej	SATA.
Obsługiwane obudowy	Wszystkie formaty: 2280 / 2260 / 2242.
Typ i liczba złączy	M-key, 2 gniazda.
Dołączone do karty rozszerzeń nośniki	2 nośniki M.2 2280 klasy enterprise. Nośniki muszą być obsługiwane przez serwer plików, zgodnie z wytycznymi firmy Synology wskazanej na stronie internetowej https://www.synology.com/pl-pl/compatibility.
Stan	Fabrycznie nowe, nieotwierane i nieużywane przed dniem dostarczenia. Muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
Rodzaj nośnika	Półprzewodnikowy SSD.
Pojemność	Minimum 480 GB.
Wydajność	Minimum odczyt sekwencyjny 500 MB/s. Minimum zapis sekwencyjny 400 MB/s.
Interfejs	SATA 6G (trzeciej generacji).
Typ	M.2 2280.
Klasyfikacja wytrzymałości (zapisy w okresie istnienia)	Minimum 1 PBW.
Nominalny czas pracy	Minimum 2 000 000 godzin.
Warunki gwarancji	**Dotyczy jednostki z zainstalowanymi nośnikami:** Minimum 60-miesięczna Gwarancja Producenta z gwarancją wymiany uszkodzonego sprzętu następnego dnia roboczego (tzw. NBD). Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. **Dotyczy karty rozszerzeń M.2 SSD:** Minimum 36-miesięczna Gwarancja Producenta. **Dotyczy nośników do karty rozszerzeń:** Minimum 60-miesięczna Gwarancja Producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.

Informacje szczegółowe dotyczące przedmiotu zamówienia dla części 3: 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).
		FUNKCJONALNOŚĆ PUNKTOWANA W RAMACH KRYTERIÓW OCENY OFERT: System jest objęty serwisem gwarancyjnym producenta przez okres **60 miesięcy**, polegającym na naprawie zgłoszonych usterek i awarii lub wymianie urządzenia w przypadku jego wadliwości, która uniemożliwia naprawę. W ramach tego serwisu producent zapewnia 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.