Załącznik nr 2 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Stacje robocze

Dostawa i instalacja 4 komputerów typu All-in-One

Ilość sztuk	4
Rodzaj	All-In-One
Kolor obudowy	Czarny
Przekątna ekranu	Min. 23,8
Waga	Max. 7 kg
Proporcje ekranu	16:9
Rozdzielczość ekranu	Min. 1920 x 1080 px
Procesor	Taktowanie: min. 2 GHz Ilość rdzeni / wątków: min. 2 / 4 Pamięć Cache: min. 4 MB Procesor uzyskujący w teście wydajności PassMark CPU Mark minimum 4800 pkt. na dzień 14.10.2022 r
Pamięć RAM	Zainstalowana pamięć RAM: min. 8 GB Maks. wielkość pamięci: min. 16 GB Liczba obsadzonych gniazd pamięci: 1 Liczba wolnych gniazd pamięci: min. 1
Dysk	Typ dysku: SSD Pojemność SSD: min. 240 GB Format szerokości SSD: M.2 Interfejs dysku SSD: PCI-Express Możliwość rozbudowy o dodatkowy dysk 2,5”
Interfejs sieciowy	1 x RJ45 100/1000 Mbit/s WiFi Bluetooth min. 5.0
Porty	Minimalnie: 1 x HDMI 1 x RJ45 10/100/1000 Mbit/s 2 x USB 2.0 2 x USB 3.2 1 x Audio
System operacyjny	Windows 10 Pro lub równoważny Zamawiający wymaga, aby klucz licencyjny systemu operacyjnego był zaszyty w BIOS. Nie dopuszcza się systemu typu REFURBISHED

Gwarancja	Okres gwarancji: min. 3 lata
Akcesoria w zestawie	Klawiatura Mysz
Dodatkowe informacje	Diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera. Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek – możliwość kontaktu przez telefon, formularz web lub chat online. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.
Uwagi	Zamawiający nie dopuszcza stosowania adapterów i przejściówek w celu uzyskania zapisanych w specyfikacji wymagań dotyczących komputerów. Instalacja oprogramowania wraz z konfiguracją konta domenowego.

Dostawa i instalacja 1 laptopa 17”

Ilość sztuk	1
Rodzaj	Laptop
Przekątna ekranu	Min. 17’’
Waga	Max. 2,5 kg
Rozdzielczość ekranu	Min. 1920 x 1080 px
Procesor	Taktowanie: min. 2,3 GHz Ilość rdzeni / wątków: min. 4 / 8 Pamięć Cache: min. 8 MB Procesor uzyskujący w teście wydajności PassMark CPU Mark minimum 10000 pkt. na dzień 14.10.2022 r
Pamięć RAM	Zainstalowana pamięć RAM: min. 8 GB Maks. wielkość pamięci: min. 16 GB Liczba wolnych gniazd pamięci: min. 1 Rodzaj pamięci: SODIMM DDR4 Częstotliwość szyny pamięci: min. 3200 MHz
Dysk	Typ dysku: SSD Pojemność SSD: min. 240 GB Format szerokości SSD: M.2
Interfejs sieciowy I bluetooth	WiFi 6 11ax, 2x2 + BT5.1
Porty	Minimalnie: 1x USB 2.0 1x USB 3.2 Gen 1 1x USB-C 3.2 Gen 1 1x HDMI 1.4b 1x CardReader
Kamera	Min. 720p

Głośniki	Stereo min. 1.5W x2, Dolby Audio
System operacyjny	Windows 10 Pro lub równoważny Zamawiający wymaga, aby klucz licencyjny systemu operacyjnego był zaszyty w BIOS. Nie dopuszcza się systemu typu REFURBISHED
Gwarancja	Okres gwarancji: min. 2 lata
Bateria	Min. 45Wh
Dodatkowe informacje	Diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera. Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek – możliwość kontaktu przez telefon, formularz web lub chat online. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.
Uwagi	Zamawiający nie dopuszcza stosowania adapterów i przejściówek w celu uzyskania zapisanych w specyfikacji wymagań dotyczących komputerów. Instalacja oprogramowania wraz z konfiguracją konta domenowego.

Scaner

Dostawa i instalacja Scanera

Ilość sztuk	1
Typ skanera	Płaski z podajnikiem ADF
Rozdzielczość optyczna:	Min. 600 x 600 dpi
Skanowane rozmiary	A4
Szybkość skanowania:	Monochromatyczny: min. 24 strony Kolor: min. 24 strony
Interfejs	USB
Tryb skanowania	Jednoprzebiegowy
Duplex	Automatyczny
Pojemność podajnika	Min. 50 stron
Poziom hałasu	Max. 56 dB
Gwarancja	Min. 12 miesięcy

Serwer

Dostawa serwera Rack 19” z serwerowym systemem operacyjnym do obsługi Serwera Terminali z instalacją i konfiguracją.

Ilość sztuk	1
Obudowa	Rack max. 2U

	Głębokość max. 750 mm.
Płyta główna	Obsługa min. 2 CPU
Procesory	Ilość: min. 1 szt. Taktowanie bazowe: min. 2.30 GHz Ilość rdzeni / wątków: min. 16/32 Pamięć Cache: min. 24 MB Pobór mocy: max. 150 W Procesor uzyskujący w teście wydajności PassMark CPU Mark minimum 30000 pkt. na dzień 22.09.2022 r
Pamięć RAM	TYP: DDR 4 Rodzaj: RDIMM Pojemność: min. 2x16 GB
Kontroler RAID	Rodzaj: sprzętowy Pamięć cache: min. 8 GB Poziomy RAID: 0/1/5/6/10/50/60 Rodzaje dysków: SAS/SATA
Dyski twarde	Ilość: min. 2 szt. Interfejs: HDD SAS 12 Gb/s Prędkość obrotowa: min. 10000 obr/min Pojemność każdego z dysków: min. 500 GB Typ obudowy: Hot Plug
Karta sieciowa	Zintegrowana Min. 2 porty RJ45 GbE
Zdalne zarządzanie	Zintegrowana funkcja serwera – zdalne zarządzanie serwerem po adresie IP z opcją zdalnego wyłączania i uruchomienia serwera.
Optymalizacja rozruchu	Kontroler z min. 2 dyskami M.2 o pojemności min. 240GB każdy (RAID1)
Zasilanie	Ilość zasilaczy HOT-PLUG: min. 2 Moc: min. 750 W każdy
Szyny montażowe	Z ramieniem na kable
System operacyjny	Microsoft Windows Server 2019 Standard wraz z dodatkowymi 5 licencjami CAL RDS dla użytkowników. (wymagany ze względu na obecnie używane środowisko serwerowe). Nie dopuszcza się systemu typu REFURBISHED
Gwarancja	Okres gwarancji: min. 3 lata Okres gwarancji na Dyski: min. 1 rok Czas reakcji: max. następny dzień roboczy
Instalacja i konfiguracja	1. Instalacja serwera w szafie Rack i podłączenie do infrastruktury sieciowej. 2. Przygotowanie RAID 1, instalacja systemu Windows serwer, podłączenie do istniejącej domeny. 3. Instalacja serwera terminali i konfiguracja 20 kont (konfiguracja aplikacji). 4. Przeniesienie danych użytkowników z komputerów lokalnych na serwer. 5. Instalacja dodatkowych programów użytkowników na serwerze (programy do obsługi Urzędu). 6. Przygotowanie backup danych serwera do istniejącej macierzy.

Pakiet biurowy OFFICE

Dostawa pakietu biurowego Microsoft Office 2021 lub równoważnego wraz z instalacją na komputerach użytkowników.

Ilość sztuk	4
Opis	Microsoft Office 2021 lub równoważny W pakiecie: Word, Excel, Powerpoint, Outlook Polska wersja językowa Licencja wieczysta

UPS

Dostawa zasilacza UPS wraz z instalacją w szafie Rack.

Ilość sztuk	1
Typ obudowy	Rack
Kolor	Czarny
Waga	Max. 25 kg
Wymiary	Max. 450 x 90 x 730
Moc pozorna	Min. 2900 VA
Moc czynna	Min. 2600 W
Liczba i pojemność akumulatorów	Min. 6 szt. 9Ah
Zabezpieczenia	Filtr przeciwprzepięciowy Filtr przeciw przeładowaniu
Porty i gniazda	Min. Porty zasilania we.: IEC-C19 Porty zasilania we.: IEC-C20 Porty zasilania wy.: 6 x IEC-C13 Gniazda we/wy: 1 x USB (Type B) Gniazda we/wy: 1 x RS-232 (COM) Gniazda we/wy: 2 x RJ-11/RJ-45
Instalacja	Instalacja UPS w szafie serwerowej, podłączenie urządzeń do UPS i jego konfiguracja do pracy serwerowej.

Router

Dostawa routera wraz z instalacją i konfiguracją w szafie Rack.

Ilość sztuk	1
Typ obudowy	Rack
Typ	xDSL
Architektura sieci	GigabitEthernet
Zasilanie	Liczba wejść DC: 2 (gniazdo DC, PoE-IN)

Procesor	Liczba rdzeni: min. 1 Częstotliwość nominalna procesora: 600 MHz
Pamięć	Rozmiar pamięci: min. 128 MB Typ pamięci: NAND
Porty	Min. Porty we/wy: 5 x 10/100/1000 Mbit/s Porty we/wy: 5 x 10/100 Mbit/s Porty we/wy: 1 x Serial port (RJ-45) Porty we/wy: 1 x USB 2.0 Type A
Instalacja i konfiguracja	1. Instalacja routera w szafie Rack 2. Konfiguracja dostępu do Internetu

Switch

Dostawa switch wraz z instalacją i konfiguracją w szafie Rack.

Ilość sztuk	1
Typ obudowy	Rack (zestaw do montażu w komplecie)
Rodzaj	Przełącznik 48 port - smart
Porty	48 x 10/100/1000 + 4 x 10 Gigabajtów SFP+
Protokół routingu	IGMPv2, IGMP, IGMPv3, MLDv2, MLD, MSTP, RSTP, STP
Protokół zdalnego zarządzania	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH, SSH-2, CLI, SCP, ICMP, DHCP, RSTP, TACACS+
Pamięć RAM	Min. 256 MB
Pamięć fleszowa	Min. 64 MB
Gwarancja	Min. 36 miesięcy
Instalacja i konfiguracja	1. Instalacja switch w szafie Rack 2. Przebudowanie sieci LAN 3. Konfiguracja VLAN

Firewall

Dostawa, instalacja i konfiguracja urządzenia Firewall wraz z 3 letnim wsparciem i aktualizacją.

Ilość sztuk	1
Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie

	odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
INTRUSION PREVENTION SYSTEM (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator 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. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

	9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
KSZTAŁTOWANIE PASMA (Traffic Shapping)	1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. 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 wykrycia infekcji.
OCHRONA ANTYSPAM	1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 3. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN

	współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator ma mieć możliwość dodawania własnych kategorii URL. 4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 7. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
UWIERZYTELNIANIE	1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może

	wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
ROUTING (TRASOWANIE)	1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
ADMINISTRACJA URZĄDZENIEM	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 6. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 7. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 8. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 9. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu

	IPFIX. 10. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 11. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 12. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
RAPORTOWANIE	1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 7. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 8. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
POZOSTAŁE USŁUGI I FUNKCJE	1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny. 5. Urządzenie ma posiadać usługę DNS Proxy. 6. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS	1. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
PARAMETRY SPRZĘTOWE	1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów. 3. Liczba portów Ethernet 10/100/1000Mbps – min.8. 4. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 5. Przepustowość Firewall (1518 bajtów UDP) – minimum 2Gbps. 6. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1.6Gbps. 7. Przepustowość filtrowania Antywirusowego – minimum 400Mbps. 8. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 350Mbps. 9. Maksymalna liczba tuneli VPN IPSec – minimum 50. 10. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20. 11. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20. 12. Obsługa interfejsów 802.11q (VLAN) – minimum 128 13. Liczba równoczesnych sesji – minimum 200 000 i nie mniej niż 15 000 nowych sesji/sekundę. 14. Urządzenie nie ma limitu na liczbę użytkowników. 15. Liczba reguł filtrowania – minimum 4 096. 16. Liczba tras statycznego routingu – minimum 512. 17. Liczba tras dynamicznego routingu – minimum 10 000.
AKTUALIZACJA MODUŁÓW	Min. 3 lata dla modułów FW+IPS, VPN, filtr URL, AV, AS
INSTALACJA I KONFIGURACJA	1. Instalacja urządzenia w szafie serwerowej 2. Podłączenie urządzenia do sieci 3. Konfiguracja urządzenia (w tym VPN dla użytkowników)

Przeprowadzenie szkoleń dla pracowników Urzędu Gminy Dąbrowice

1. Szkolenia zostaną przeprowadzone w formie stacjonarnej (w siedzibie Zamawiającego) w formie wykładu i części praktycznej **dla dwóch grup maksymalnie 12 osobowych.**
2. Tematyka szkolenia będzie dotyczyła w szczególności następujących zagadnień:
   a) bezpieczeństwo pracy zdalnej i bezpieczeństwo pracy przez pulpity zdalne, m.in:
   - zagrożenia dla użytkownika i zasobów organizacji;
   - socjotechniczne mechanizmy działania cyberprzestępców;
   - rozpoznawanie zagrożeń oraz reagowanie na pojawiające się niebezpieczeństwa;
   - dobre praktyki zabezpieczania się przed poszczególnymi zagrożeniami;

- utrzymanie bezpieczeństwa informacji w systemach informatycznych (zabezpieczanie środowiska pracy)
- podstawy bezpieczeństwa systemów informatycznych;
- przenoszenie się zagrożeń pomiędzy obszarem prywatnym a służbowym;
- profilaktyka bezpiecznego korzystania z Internetu oraz sieci LAN i Wi-Fi,
- konsekwencje lekceważenia zasad cyberbezpieczeństwa.

Czas trwania szkolenia łącznie 14 h – po 7 godzin na grupę.

b) obsługa programu EXCEL na poziomie zaawansowanym.

Czas trwania szkolenia łącznie 10 h – po 5 godzin na grupę.

Zamawiający wymaga, aby montaż i konfiguracja sprzętu wskazanego w opisie przedmiotu zamówienia odbywał się poza godzinami pracy Urzędu Gminy w Dąbrowicach tj. godziny 7:30-15:30.

Zamawiający wymaga, aby prace konfiguracyjne i instalacyjne odbywały się siedzibie zamawiającego w godzinach 16:00 – 19:00 od poniedziałku do piątku, natomiast w dni wolne od pracy w godzinach: 9:00-11:00.

Harmonogram prac wykonawcy wymaga zgody ze strony zamawiającego.