Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Szczegółowy opis przedmiotu zamówienia do zadania:

Zakup i dostawa sprzętu informatycznego do Urzędu Miasta i Gminy Nowa Dęba w ramach realizacji projektu grantowego „Cyfrowa Gmina”

Zakup i dostawa sprzętu informatycznego do Urzędu Miasta i Gminy Nowa Dęba w ramach realizacji projektu grantowego „Cyfrowa Gmina”.

Zakup i dostawa: 50 zestawów komputerowych wraz z monitorami – 50 szt. oprogramowania biurowego – 50 szt.

1) Zestaw Komputerowy – 50 sztuk

Stacja robocza	
Nazwa komponentu	**Charakterystyka (wymagania minimalne)**
Typ	*Komputer stacjonarny w obudowie Small Form Factor. W ofercie wymagane jest podanie modelu, symbolu oraz producenta*
Zastosowanie	*Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej*
Dostawa	*Dostawa fabrycznie nowego zestawu komputerowego do siedziby zamawiającego, własnym transportem, na własny koszt, własne ryzyko i złożonych w miejscu wskazanym przez Zamawiającego. Produkt przeznaczony na rynek europejski,* zapakowany w oryginalne opakowanie
Procesor	*Minimum 4-rdzeniowy, minimum 3.70GHz, osiągający w teście PassMark CPU wynik minimum 8800 pkt.*
BIOS	*Możliwość odczytania z BIOS:* *1. Wersji BIOS* *2. Modelu procesora, prędkości procesora*

	3. *Informacji o ilości pamięci RAM wraz z informacją o jej prędkości i technologii wykonania, a także o pojemności*
Pamięć operacyjna	*1 x 8GB 2666 MHz możliwość rozbudowy do mib. 32GB, minimum jeden sloty wolny na dalszą rozbudowę*
Parametry pamięci masowej	*Min. 256GB m.2 2280 PCIe NVMe. Możliwość instalacji dodatkowych dwóch dysków 2,5".*
Grafika	*Zintegrowana z płytą główną, ze wsparciem dla DirectX 12, OpenGL 4.5 oraz dla rozdzielczości 4096x2304@60Hz osiągająca w teście Average G3D Mark wynik na poziomie 1290 punktów.*
Wyposażenie multimedialne	*Karta dźwiękowa zintegrowana z płytą główną; wbudowany głośnik*
Obudowa	*Obudowa typu Small Form Factor o maksymalnej sumie wymiarów 66,8 cm posiadająca min. 1 szt półki zew 5,25" na napęd optyczny typu SLIM i 1 wewnętrzne miejsce na montaż dysku 3,5" lub 2 x 2,5". Obudowa zabezpieczona przed przypadkowym otwarciem jedną śrubą radełkową. Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producent. Waga komputera max 4,0 kg. Z przodu obudowy wymagany jest wbudowany fabrycznie wizualno-dźwiękowy system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej: – awarie procesora lub pamięci podręcznej procesora – uszkodzenie lub brak pamięci RAM, – uszkodzenie płyty głównej Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona). Zasilacz o mocy max 180W z aktywnym PFC i sprawności min 90%*
Zgodność z systemami operacyjnymi i standardami	*Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym Windows 10 64-bit (załączyć wydruk ze strony Microsoft WHCL lub oświadczenie producenta).*
Bezpieczeństwo	1. *Komputer wspierający standard Trusted Platform Module (TPM v 2.0) (firmware)* 2. *Możliwość zapięcia linki typu Kensington w dedykowanym standardowym slocie* 3. *Oczko z tyłu obudowy na zapięcie kłódki lub linki* 4. *Czujnik otwarcia obudowy*
Certyfikaty standardy	*- Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)* *– Deklaracja zgodności CE (załączyć do oferty)*

Ergonomia	*Maksymalnie 28 dB z pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; wymaga się dostarczenia odpowiedniego certyfikatu lub deklaracji producenta*
Warunki gwarancji	*3-letnia gwarancja producenta świadczona na miejscu u klienta Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem*
Wsparcie techniczne producenta	*Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: - weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć) - czasu obowiązywania i typ udzielonej gwarancji. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera*
System operacyjny	• *Preinstalowany przez producenta system operacyjny w języku polskim z pełną obsługą platformy .NET.* • *Wbudowane graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.* • *Wbudowany system pomocy w języku polskim.* • *Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.* • *Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).* • *Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.*

	• *Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i v6.* • *Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.* • *Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).* • *Wsparcie dla PowerShell – możliwość uruchamiania interpretera poleceń.* • *Możliwość ustanowienia polityki złożoności haseł logowania, wymuszania cyklicznej zmiany hasła.* *Zamawiający nie dopuszcza systemu z rynku wtórnego, lub instalowanego przez wykonawcę, a także systemów w wersjach testowych lub edukacyjnych.*
Wymagania dodatkowe	*1. Wbudowane porty i złącza:* *- porty wideo: min. 1 szt. VGA i 1 szt. HDMI* *- min. 8 x USB w tym min:* *4 porty USB 3.1 z przodu obudowy oraz 4 porty USB 2.0 z tyłu obudowy* *- port sieciowy RJ-45,* *- porty audio COMBO – z przodu obudowy* *- port liniowy audio stereo - wejście i wyjście z tyłu obudowy* *- 1 x czytnik kart SD* *Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.* *2. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana).* *3. Płyta główna wyposażona w:* *- 2 złącza DIMM z obsługą do 32GB pamięci RAM 2666MHz każde z nich* *- slot M.2 dla karty WiFi z kartą* *- slot M.2 dla pamięci masowej 2242/2280* *1 x PCIe x16* *1 x PCIe x1* *4. Bezprzewodowa karta sieciowa ac 1x1 +Bluetooth 4.2.* *5. Klawiatura USB w układzie polski programisty.*

	6. Mysz optyczna USB z min. dwoma klawiszami oraz rolką (scroll). *7. Nagrywarka SATA DVD SLIM wbudowana w komputer.*
Oprogramowanie dodatkowe – pakiet biurowy	*Licencje pakietu biurowego spełniające następujące wymagania techniczne:* *1. Wymagania odnośnie interfejsu użytkownika:* *a. pełna polska wersja językowa interfejsu użytkownika,* *b. prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;* *2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:* *a. posiada kompletny i publicznie dostępny opis formatu,* *b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012, poz. 526);* *3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji;* *4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy);* *5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;* *6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:* *a. edytor tekstów,* *b. arkusz kalkulacyjny,* *c. narzędzie do przygotowywania i prowadzenia prezentacji,* *d. narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),* *e. narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR;* *7. Edytor tekstów musi umożliwiać:* *a. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,* *b. wstawianie oraz formatowanie tabel,* *c. wstawianie oraz formatowanie obiektów graficznych,* *d. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),* *e. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,* *f. automatyczne tworzenie spisów treści,* *g. formatowanie nagłówków i stopek stron,*

	h. *śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,* i. *nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,* j. *określenie układu strony (pionowa/pozioma),* k. *wydruk dokumentów,* l. *wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,* m. *pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word 2003 lub Microsoft Word 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,* n. *zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,* o. *wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,* p. *wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa;* 8. *Arkusz kalkulacyjny musi umożliwiać:* a. *tworzenie raportów tabelarycznych,* b. *tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,* c. *tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,* d. *tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService),* e. *obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,* f. *tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,* g. *wyszukiwanie i zamianę danych,* h. *wykonywanie analiz danych przy użyciu formatowania warunkowego,* i. *nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,* j. *nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,*

	k. *formatowanie czasu, daty i wartości finansowych z polskim formatem,* l. *zapis wielu arkuszy kalkulacyjnych w jednym pliku,* m. *zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,* n. *zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;* 9. *Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:* a. *przygotowywanie prezentacji multimedialnych,* b. *prezentowanie przy użyciu projektora multimedialnego,* c. *drukowanie w formacie umożliwiającym robienie notatek,* d. *zapisanie jako prezentacja tylko do odczytu,* e. *nagrywanie narracji i dołączanie jej do prezentacji,* f. *opatrywanie slajdów notatkami dla prezentera,* g. *umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,* h. *umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,* i. *odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, możliwość tworzenia animacji obiektów i całych slajdów,* j. *prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,* k. *pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013;* 10. *Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:* a. *pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,* b. *przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,* c. *filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,* d. *tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,* e. *automatyczne grupowanie poczty o tym samym tytule,* f. *tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,* g. *oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,* h. *mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,*

	i. zarządzanie kalendarzem, *j. udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,* *k. przeglądanie kalendarza innych użytkowników,* *l. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,* *m. zarządzanie listą zadań,* *n. zlecanie zadań innym użytkownikom,* *o. zarządzanie listą kontaktów, p) udostępnianie listy kontaktów innym użytkownikom,* *p. przeglądanie listy kontaktów innych użytkowników,* *q. możliwość przesyłania kontaktów innym użytkowników.*

2) Monitor/wyświetlacz – 50 sztuk

Monitor / Wyświetlacz	
OBRAZ	
Parametry	**Charakterystyka (wymagania minimalne)**
Przekątna	23.8”,60.5
Panel	AMVA LED, matowe wykończenie
Rozdzielczość fizyczna	1920 x 1080 @75Hz (HDMI&DisplayPort, 2.1 megapixel Full HD)
Format obrazu	16:9
Jasność	250 cd/m^2
Kontrast statyczny	3 000:1
Kontrast ACR	80M:1
Czas reakcji (GTG)	4ms
Kąty widzenia	poziomo/pionowo: 178°/178°, prawo/lewo: 89°/89°, góra/dół: 89°/89°
Kolory	16.7mln 8bit (sRGB: 99%; NTSC: 72%)
Synchronizacja pozioma	30-80kHz
Plamka	0.275mm

INTERFEJSY/ZŁĄCZA/STEROWANIE	
Parametry	**Charakterystyka (wymagania minimalne)**
	VGAx1 HDMIx1
Wejście sygnału	DisplayPortx1
USB HUB	x2 (v.2.0)
HDCP	Tak
Wyjście słuchawkowe	tak
WŁAŚCIWOŚCI	
Parametry	**Charakterystyka (wymagania minimalne)**
Redukcja niebieskiego światła	Tak
Flicker free	tak
Wbudowane głośniki	2 x 2W
Udogodnienia	kompatybilny z Kensington-lock™, DDC2B, Mac OSX
MECHANICZNE	
Parametry	**Charakterystyka (wymagania minimalne)**
Kąt pochylenia	22° w górę; 5° w dół
Standard VESA	100 x 100mm
AKCESORIA W ZESTAWIE	
Parametry	**Charakterystyka (wymagania minimalne)**
Kable	Zasilający, USB, HDMI
ZARZĄDZANIE ENERGIĄ	
Parametry	**Charakterystyka (wymagania minimalne)**
Zasilacz	wewnętrzny

Zasilanie	AC 100 - 240V, 50/60Hz
Zużycie energii	26W typowo, 0.33W stand by, 0.29W off mode
ZRÓWNOWAŻONY ROZWÓJ	
Parametry	**Charakterystyka (wymagania minimalne)**
Certyfikaty	TCO Certified, CE, TÜV-GS, EAC, VCCI-B, RoHS support, ErP, WEEE, REACH
Klasa efektywności energetycznej	A+
Klasa efektywności energetycznej (Regulation (EU) 2017/1369	E

3) UTM

Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

	3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5. 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 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje 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. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • 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. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia 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. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

	2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.