Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 4 do SWZ. Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. Dostawa sprzętu serwerowego i sieciowego z oprogramowaniem i usługami wdrożeniowymi dla Gminy Orły w ramach projektu „Cyfrowa Gmina”

1. Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

Przedmiot dostawy	Ilość
Serwery z systemami operacyjnymi i oprogramowaniem do wirtualizacji	2
Macierz dyskowa	1
Serwerowy zasilacz awaryjny	1
Urządzenie NAS (backup)	1
Przełączniki sieciowe	3
Urządzenie UTM	1
Usługi wdrożeniowe	1

Kody CPV:

- 48820000-2 Serwery
- 30233000-1 Urządzenia do przechowywania i odczytu danych

- 31682530-4 Awaryjne urządzenia energetyczne
- 32420000-3 Urządzenia sieciowe
- 48000000-8 Pakiety oprogramowania i systemy informatyczne
- 48422000-2 Zestawy pakietów oprogramowania
- 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
- 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

2. Wymagania minimalne dla przedmiotu zamówienia

2.1. Serwery z systemami operacyjnymi i oprogramowaniem do wirtualizacji

Obszar wymagań	**Wymagania minimalne**
Obudowa	Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug,z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli .
Procesor	Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem uzyskujące w układzie dwuprocesorowym wynik co najmniej 33 000 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php w okresie nie wcześniej niż 14 dni przed terminem składania ofert. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 128 GB DDR4 registered. Płyta główna musi obsługiwać do 2 TB pamięci RAM DDR4 lub więcej.
Grafika	Zintegrowana karta graficzna ze złączem VGA.
Sieć	Co najmniej: 4x 1Gbit Base-T oraz 2x 10 Gbit SFP+.
Dyski twarde	Zainstalowane 2 szt. dysków SSD SATA o pojemności co najmniej 256 GB każdy.
Kontrolery dyskowe	Zainstalowany kontroler SAS RAID obsługujący poziomy 0, 1, 10, 5, 50. Zainstalowany kontroler SAS HBA posiadający 2 porty zewnętrzne umożliwiające podłączenie macierzy będącej przedmiotem zamówienia.

Porty	Co najmniej 3 zewnętrzne porty USB 3, w tym co najmniej 1 port na panelu przednim. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
Wentylacja	Redundantne wentylatory hotplug.
Zasilanie	Redundantne zasilacze hotplug o sprawności co najmniej 90% o mocy co najmniej 800 W każdy.
Diagnostyka	Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń, procesory pamięć RAM, status karty zrządzającej serwera wentylatory, zasilacze. System przewidywania / rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).
Zarządzanie	Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, posiadający dedykowany port RJ-45 GbE umożliwiający co najmniej: • zdalne zarządzanie przez przeglądarkę, • zdalny restart serwera, • szyfrowane połączenie (TLS, SSL), • przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM), • możliwość przejęcia konsoli tekstowej, • obsługę protokołu LDAP, • zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii, • zarządzanie alarmami (zdarzenia poprzez SNMP),

	• możliwość backupu i odtworzenia ustawień BIOS serwera oraz ustawień karty zarządzającej, • możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN, • możliwość konfiguracji i wykonania aktualizacji BIOS, firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej, • oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna).
Bezpieczeństwo	• Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych. • Moduł TPM 2.0.
Oprogramowanie – system wirtualizacji	Z serwerami należy dostarczyć pakiet oprogramowania przeznaczonego do wirtualizacji serwerów. Oprogramowanie do wirtualizacji serwerów będzie przeznaczone na cele utworzenia klastra wirtualizacyjnego składającego się z serwerów będących przedmiotem zamówienia. Oprogramowanie musi posiadać następujące cechy i funkcjonalności: 1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.

	4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi umożliwiać obsługę i wykorzystanie procesorów fizycznych wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. 6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows Server 2008, Windows Server 2012, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X. 13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.

	15. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. 16. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. 17. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 18. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 19. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 20. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. 21. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 22. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 23. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
System operacyjny	System operacyjny spełniający nw. wymagania minimalne:

	1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

	10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.

	20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych.

	c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i) Dystrybucję certyfikatów poprzez http ii) Konsolidację CA dla wielu lasów domeny, iii) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

	i) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii) Obsługi 4-KB sektorów dysków iv) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi) Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim. Zaoferowane wraz z serwerami licencje na system operacyjny: 1. muszą obejmować najnowszą wersję systemu dostępną na dzień składania oferty,

	2. łącznie muszą uprawniać do zainstalowania tego systemu na co najmniej czterech serwerach wirtualnych w klastrze wirtualizacyjnym składającym się z dwóch serwerów fizycznych będących przedmiotem zamówienia, 3. łącznie muszą obejmować licencje dostępowe dla 50 użytkowników. Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim).
Warunki gwarancyjne	Co najmniej trzyletnia gwarancja producenta, obejmująca wszystkie komponenty serwera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez infolinię lub portal producenta.

2.2. Macierz dyskowa

Obszar wymagań	**Wymagania minimalne**
Obudowa, możliwości rozbudowy macierzy	1) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maksymalnie 2U w tej szafie. 2) Obudowa pojedynczego modułu rozwiązania – półka dyskowa, moduł kontrolerów - musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia, umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy. 3) Macierz musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy. 4) Macierz nie może zawierać elementów typu bateria/akumulator wymagających jakiegokolwiek reżimu obsługowego: wymiana, przełączanie, ładowanie (np. nie dopuszcza się podtrzymania bateryjnego cache kontrolerów itp.).

	5) Rozbudowa o dodatkowe moduły dyskowe (półki dyskowe) dla obsługiwanych dysków musi odbywać się wyłącznie poprzez zakup takich modułów tj. bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy. 6) Połączenia pomiędzy półkami dyskowymi muszą zapewniać brak pojedynczego punktu awarii.
Pojemność	1) System musi umożliwiać instalację dysków wykonanych w technologii hot-plug i wyposażonych w podwójny interfejs SAS. 2) Macierz musi umożliwiać obsługę co najmniej 8 dysków SSD. 3) Zainstalowane dyski: • 4 dyski SSD-SAS 12G o pojemności co najmniej 960GB każdy oraz • 6 dysków NL-SAS 12G o pojemności co najmniej 4TB każdy.
Kontrolery	1) System musi obsługiwać 2 kontrolery pracujące w układzie nadmiarowym typu active-active i bez konieczności stosowania zewnętrznych połączeń kablowych pomiędzy nimi, z minimum 8GB pamięci podręcznej w każdym kontrolerze, wymaga się dostarczenia minimum 2 kontrolerów. 2) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik. 3) Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia. 4) Macierz musi pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach nawet w przypadku konfiguracji z jednym kontrolerem RAID. 5) W układzie z zainstalowanymi dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror. 6) Każdy z kontrolerów RAID musi posiadać dedykowane min. 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością 1 Gb/s - dla zdalnej i lokalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
Interfejsy	Minimum 2 porty SAS 12G na każdy kontroler macierzy do podłączenia serwerów.

	Należy dostarczyć 4 szt. przewodów SAS do podłączenia oferowanych serwerów.
Poziomy RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1,1+0, 5, 5+0, 6.
Wspierane dyski	Oferowany model macierzy musi wspierać dyski: 1) dyski SAS wykonane w technologii hot-plug, 2) dyski NL-SAS (NearLine SAS) wykonane w technologii hot-plug, 3) dyski SSD SAS wykonane w technologii hot-plug, 4) interfejsy obsługiwanych dysków muszą być wyposażone w minimum 2 porty pracujące w reżimie full-duplex (jednoczesna transmisję danych przez dwa porty), 5) macierz musi wspierać mieszaną konfigurację dysków SSD, SAS i NearLine SAS w obrębie pojedynczego modułu obudowy, 6) macierz musi wspierać mechanizm automatycznej przedawaryjnej migracji zapisów i składowanych danych na dysk zapasowy. 7) macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych w trybie ręcznym i automatycznym z wykorzystaniem mechanizmu typu 'time scheduler' czyli w zadanym i/lub powtarzalnym oknie czasowym. 8) macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach: - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID. 9) Macierz musi pozwalać na skonfigurowanie dowolnego dysku hot-plug dostarczonego w rozwiązaniu do roli dysku zapasowego jak w pkt.7 1) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. BackLessCopy)
Oprogramowanie, funkcjonalności	1) Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na minimum 1024 kopie migawkowych.

	2) Macierz musi wspierać VSS. 3) Macierz musi umożliwiać zdefiniowanie min. 1024 woluminów (LUN). 4) Macierz musi umożliwiać podłączenie logiczne z serwerami i stacjami poprzez minimum 4 ścieżki. 5) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek dla podłączonych stacji/serwerów. 6) Macierz musi umożliwiać rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD. 7) Oferowany model macierzy musi obsługiwać mechanizmy Thin Provisioning (przy zainstalowanych 2 kontrolerach) czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy – wymagana jest obsługa minimum 64 pól ThinProvisioning w rozwiązaniu. 8) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: - zmiana rozmiaru woluminu, - zmiana poziomu RAID, - zmiana technologii dysków dla danej grupy RAID, - dodawanie nowych dysków do istniejącej grupy dyskowej, 9) Macierz musi posiadać wsparcie dla systemu operacyjnego oferowanego wraz z serwerem oraz ewentualnie innych, które zostaną zainstalowane przez wykonawcę w ramach usług wdrożeniowych. 10) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem). 11) Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności minimum 128 TB. 12) Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowisku wirtualizacyjnym będącym przedmiotem zamówienia.

	14) Wraz z macierzą należy zapewnić dostęp do bezpłatnych aktualizacji (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego macierzy w całym okresie obowiązywania gwarancji).
Konfiguracja, zarządzanie	1) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 2) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.
Gwarancja	Co najmniej trzyletnia gwarancja producenta, obejmująca wszystkie komponenty urządzenia. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.

2.3. Serwerowy zasilacz awaryjny

Obszar wymagań	**Wymagania minimalne**
Typ urządzenia	Zasilacz awaryjny w obudowie do montażu w szafie rack, zajmujący maksymalnie 3U
Moc	Co najmniej 4500 W, moc pozorna co najmniej 5000 VA
Topologia	On-line
Czas podtrzymania	11 min. dla obciążenia 50% lub dłużej
Gniazda	Co najmniej 6 gniazd IEC 320 C13, co najmniej 4 gniazda IEC 320 C19
Komunikacja	RJ-45
Sygnalizacja	Wyświetlacz LCD lub diody LED, alarm dźwiękowy
Funkcjonalność	• aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania (wymagane wsparcie dla systemu operacyjnego oferowanego wraz z serwerami) • zarządzanie przez SNMP

	• automatyczny wewnętrzny bypass • bezprzerwowa wymiana baterii • możliwość dołączenia baterii wydłużających czas podtrzymania zasilania
Gwarancja	Co najmniej trzyletnia gwarancja producenta (bez akumulatora), co najmniej dwuletnia gwarancja producenta na akumulator

2.4. Urządzenie NAS (backup)

Obszar wymagań	**Wymagania minimalne**
Obudowa	Obudowa do montażu w szafie rack 19” o wysokości maksymalnie 2U, w komplecie z szynami do montażu
Pamięć RAM	Zainstalowane co najmniej 4 GB pamięci RAM. Możliwość rozbudowy do 32 GB pamięci RAM lub więcej.
Obsługa dysków	Ilość kieszeni dysków: co najmniej 8 (możliwość rozbudowy do 12 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 12 dysków). Obsługiwane typy dysków: 3,5” SATA HDD, 2,5” SATA HDD, 2,5” SATA SSD Możliwość zainstalowania karty SSD M.2.
Zamontowane dyski	Zamontowane co najmniej 6 dysków o pojemności co najmniej 8 TB każdy, o prędkości obrotowej co najmniej 7200 rpm, prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin.
RAID	Obsługa RAID co najmniej: pojedynczy dysk, RAID 0, 1, 5, 6, 10, JBOD
Porty	Wbudowany interfejs 1Gbit/s z min. czterema portami RJ-45 oraz funkcją agregacji łączy. Porty USB 3.0 – co najmniej 2 szt. Port eSATA – co najmniej 1 szt.
Oprogramowanie	• Panel użytkownika i oprogramowanie dostępne w pełnej polskiej wersji językowej. • Urządzenie musi być wyposażone w zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z oferowanym

	serwerowym systemem operacyjnym oraz maszyn wirtualnych uruchomionych w oparciu o oferowane oprogramowanie do wirtualizacji. • Urządzenie musi posiadać centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych. • Oprogramowanie do backupu musi umożliwiać szybkie przywracanie plików, całych maszyn fizycznych i maszyn wirtualnych. • Wbudowane systemy zabezpieczeń sieciowych, antywirus, szyfrowanie AES256bit oraz dwustopniowe uwierzytelnianie użytkowników. • Ochrona za pomocą funkcji kopii zapasowych, jednostek LUN, migawek, klonowania i synchronizacji danych. • Wbudowany serwer FTP z funkcjami SSL, TLS.
Gwarancja	Gwarancja na urządzenie wraz z dyskami co najmniej 24 miesiące.

2.5. Przełączniki sieciowe

Obszar wymagań	**Wymagania minimalne**
Typ urządzenia	Przełącznik wielowarstwowy L2/L3, zarządzany
Obudowa	Do montażu w szafie rack 19”, wysokość 1U
Porty	48 portów 10/100/1000BaseT RJ-45, uplink 4 x 10G SFP+ Port konsoli USB Type-B/RJ45 Porty dostępowe przełącznika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
Funkcjonalność	Obsługa protokołu NTP Funkcje DHCP server, DHCP relay Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping Blokowanie Head of Line (HOL) Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD) Zapobieganie atakom DoS

	Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6 Obsługa funkcji Plug & Play Przycisk reset
Wydajność	Przepustowość przełącznika (switching bandwidth) 170 Gb/s Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 130 Mpps Pamięć DRAM – 512 MB
Obsługa standardów komunikacyjnych	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet
Zarządzanie	Port konsoli Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją Obsługa protokołów SNMPv3, SSHv2, https, syslog Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgrade'u oprogramowania urządzenia Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki Obsługa protokołu LLDP i LLDP-med.
Gwarancja	Co najmniej trzyletnia gwarancja producenta.

2.6. Urządzenie UTM

Obszar wymagań	**Wymagania minimalne**

Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi wspierać 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 – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, przestrzeń dyskowa	1. System realizujący funkcję firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45 i 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System realizujący funkcję firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB

Wydajność	1. W zakresie frewall'a obsługa nie mniej niż 1,4 tys. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość stateful firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 6. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 7. 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 1.4 Gbps. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
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: 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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 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. 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.

	11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
Polityki firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. 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. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować 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 • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
Połączenia VPN	1. 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. 2. 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. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
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.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

	5. 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. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej adresy URL pogrupowane w kategorie tematyczne. 2. 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. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall 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. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

	6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. 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. 2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 3. Musi istnieć możliwość logowania do serwera SYSLOG.
Licencje	Z urządzeniem należy dostarczyć licencje upoważniające do korzystania na urządzeniu z aktualnych baz funkcji ochronnych producenta i serwisów przez co najmniej trzy lata w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, bazy reputacyjne adresów IP/domen.
Gwarancja	Co najmniej trzyletnia gwarancja producenta.

2.7. Usługi wdrożeniowe

W ramach zamówienia Wykonawca zrealizuje usługi instalacji i konfiguracji zakupionego sprzętu i oprogramowania oraz przeniesienia oprogramowania i baz danych ze dotychczas eksploatowanych serwerów.

Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.

Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.

Zamawiający wymaga wykonania następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:

1) Sporządzenia planu wdrożenia, według którego nastąpi jego realizacja. Plan ten musi być uzgodniony z Zamawiającym i uwzględniać wszystkie aspekty wdrożenia. W szczególności:
    a. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych;
    b. schematy połączeń;
    c. mechanizmy działania głównych elementów sprzętowych;
        i. sieć LAN,
        ii. klaster wirtualizacyjny,
        iii. system backupu i archiwizacji danych,
        iv. system serwerowy,
        v. system macierzowy,
        vi. firewall (urządzenie UTM);
    d. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności;
    e. sposób odbioru uzgodniony z Zamawiającym;
    f. listę i opisy procedur, stosowanie których gwarantuje Zamawiającemu prawidłowe działanie systemu;
    g. opis przypadków, w których projekt dopuszcza niedziałanie systemu.

Montaż i fizyczne uruchomienie systemu

Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:

2) Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniu wskazanym przez Zamawiającego.
3) Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
4) Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
5) Podłączenie wszystkich elementów do infrastruktury Zamawiającego.
6) Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.

7) Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
8) Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
9) Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
10) Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:
    a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
    b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.
    c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
    d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
11) Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji.
12) Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych" – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów)
13) Urządzenie NAS należy przyłączyć do infrastruktury Zamawiającego celem stworzenia miejsca na przechowywanie danych backupu.

Instalacja i konfiguracja oprogramowania

14) Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji.
15) Instalacja i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych.
16) Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego).
17) Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych.

Konfiguracja sieci LAN

18) Konfiguracja dostarczanych przełączników w zakresie:
    a. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
    b. Stworzenia odpowiednich konfiguracji STACK.
    c. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).

d. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.
    i. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink.
    ii. Z wykorzystaniem połączeń światłowodowych oraz miedzianych.
    iii. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu.
    iv. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps.
e. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.
f. Konfiguracja routingu pomiędzy sieciami VLAN na urządzeniu UTM.
g. Testowanie obsługi ruchu sieciowego.
h. Testowanie skuteczności zabezpieczeń.

Konfiguracja elementów bezpieczeństwa sieciowego

19) Urządzenie firewall - konfiguracja urządzenia UTM w nw. zakresie.
    a. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
    b. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
    c. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, kontrola aplikacji, filtrowanie WWW, filtrowanie e-mail).
    d. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu.
    e. Konfiguracja dostarczonych systemów firewall:
        i. Konfiguracja podstawowych parametrów;
        ii. Konfiguracja translacji adresów NAT;
        iii. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze itp.;
        iv. Konfiguracja inspekcji określonych protokołów sieciowych;
        v. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
        vi. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
        vii. Testowanie działania bramy.
    f. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
        i. Konfiguracja podstawowych parametrów

   ii. Konfiguracja mechanizmów ochrony określonych; sieci VLAN przez moduł wykrywania włamań;
   iii. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
   iv. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
   v. Testowanie działania ochrony IPS.

g. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
   i. Przypisanie adresu IP do zarządzania;
   ii. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3;
   iii. Definicja reguł filtrowania/blokowania;
   iv. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny.
h. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.
i. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.
j. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.
k. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC
l. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
   i. kontrola dostępu - zapora ogniowa klasy Stateful Inspection;
   ii. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar;
   iii. ochrona przed atakami - Intrusion Prevention System [IPS/IDS];
   iv. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM;
   v. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP);
   vi. kontrola pasma oraz ruchu [QoS, Traffic shaping];
   vii. Kontrola aplikacji oraz rozpoznawanie ruchu P2P;
   viii. Ochrona przed wyciekiem poufnej informacji (DLP);

ix. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL);
x. Inspekcja ruchu SSL;
xi. Ochrony przez atakami na stacje klienckie;
xii. Kontrola pasma.

m. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi (np.: RCIM).
n. Konfiguracja logowania i raportowania.

Serwer SMTP

20) Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.
21) Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z urządzeń sieciowych, serwerów, macierzy dyskowej, oprogramowania do tworzenia kopii zapasowych, oprogramowania do wirtualizacji oraz aplikacji.
22) Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.

Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych

23) Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy.
24) Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego).
25) Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie.
26) Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.

Uruchomienie środowiska wirtualizacyjnego

Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:

27) Aktywacja licencji dostarczonego oprogramowania do wirtualizacji na stronie producenta.

28) Przygotowanie serwerów do instalacji oprogramowania do wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
29) Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
30) Instalacja oprogramowania do wirtualizacji na dostarczonych serwerach.
31) Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania do wirtualizacji oraz przez producenta serwerów.
32) Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) (n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
33) Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Zamawiającego. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) (n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
34) Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
35) Przygotowanie koncepcji wirtualizacji fizycznych maszyn.
36) Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
37) Konfiguracja klastra wysokiej dostępności:
    a. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
    b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
    c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
38) Weryfikacja działania klastra wysokiej dostępności.
39) Migracja istniejącej infrastruktury do środowiska wirtualnego.
40) Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową
41) Konfiguracja powiadomień o krytycznych zdarzeniach (e-mail).

System kopii zapasowych (backupu)

42) Instalacja oprogramowania do tworzenia kopii zapasowych dostarczonego w pakiecie z urządzeniem NAS.
43) Aktywacja oraz instalacja niezbędnych licencji.
44) Konfiguracja stacji zarządzającej.
45) Dołączenie klientów do systemu backupu.
46) Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:
    a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
    b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
    c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
    d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową.
47) Zdefiniowanie powiadomień o przebiegu zadania oraz o zdarzeniach (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres e-mail).
48) Uruchomienie testowych zadań backupu.
49) Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email.
50) Uruchomienie testowych zadań odtworzenia danych.
51) Miejscem przechowywania kopii zapasowych ma być dostarczane urządzenie NAS.
52) Na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym.
53) System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na urządzeniu NAS.

Usługa katalogowa

54) Wymagane zaplanowanie liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików zapewniającej, w przypadku awarii pojedynczego serwera, ciągły dostęp do usługi katalogowej, a w szczególności do mechanizmów uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym.
55) Instalacja systemu operacyjnego serwerów. Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.

56) Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.
57) Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.
58) Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:
    a. Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości;
    b. Śledzenie zmian dotyczących tworzenia, usuwania obiektów.
59) Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
60) Konfiguracja globalnej polityki haseł dla domeny.
61) Konfiguracja polityki haseł dla kadry zarządzającej.
62) Szczegółowe dane zostaną przekazane na etapie konfiguracji.
63) Stworzenie skryptów służących do tworzenia struktury usługi katalogowej. Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje opracowanie przez Wykonawcę skryptów ułatwiających te zadania.
64) Opracowane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące ich działanie. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi.
65) Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.
66) Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows.
67) Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby:
    a. Z wykorzystaniem skryptów logowania.
    b. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows 10 i nowszych. Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie.

Uruchomienie i skonfigurowanie serwera plików oraz wydruków

68) Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:
    a. Replikację multi-master z rozwiązywaniem konfliktów;
    b. Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.
69) Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.
70) Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów.
71) Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.
72) Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego.
73) Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych.
74) Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji.
75) Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:
    a. Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder;
    b. Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder;
    c. Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.
76) Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.

Serwery uwierzytelniające

77) Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych.
78) Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.
79) Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę.
80) Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.
81) Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.

Dołączenie stacji roboczych do domeny

82) Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny (50 stacji roboczych). W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).
83) Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów według założeń:
    a. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet;
    b. Administrator zatwierdza aktualizacje do instalacji;
    c. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu.
84) Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:
    a. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje;
    b. Kategorii aktualizacji;
    c. Grup komputerów;
    d. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów;
    e. Zasad automatycznego zatwierdzania nowych aktualizacji;

f. Mechanizmów raportowania (e-mail).

Przygotowanie infrastruktury PKI

85) Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 8.x, Windows 10 i Windows 11.
86) Wymagana przez Zamawiającego konfiguracja musi uwzględniać:
    a. Zaplanowanie i uruchomienie wewnętrznej struktury CA;
    b. Konfigurację szablonów certyfikatów;
    c. Wydanie certyfikatów dla serwerów oraz stacji roboczych;
    d. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów;
    e. Wskazanie wszystkich możliwych dróg publikacji list CRL;
    f. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji.

Testowanie i modyfikacja parametrów infrastruktury sieciowej

87) Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego.
88) Testowanie wydajności przesyłu i zapisu danych do środowiska LAN.
89) Testowanie mechanizmów replikacji danych.
90) Testowanie dostępu publicznego do zasobów.
91) Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu.
92) Testowanie autoryzowanego dostępu do wewnętrznych zasobów.
93) Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach.

Migracja systemów informatycznych

94) Wykonawca przeniesie obecnie eksploatowane systemy informatyczne na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Systemy wraz z ich bazami danych muszą zostać przeniesione na nowe zasoby serwerowo-macierzowe.
95) W ramach migracji zostaną przeniesione nw. systemy:
    Oprogramowanie Biura Usług Komputerowych Softres, Rzeszów
    a. Moduł obsługi podatkowej wraz z księgowością podatkową
    b. Moduł ewidencji zwrotu podatku akcyzowego

c. Moduł obsługi podatku od środków transportowych
d. Moduł obsługi opłat za gospodarowanie opłatami komunalnymi
e. Moduł finansowo-księgowy
f. Moduł kasowy
g. Moduł kadry
h. Moduł ewidencja środków trwałych
i. Moduł system ewidencja i rozliczanie opłat
j. Broker komunikacyjny SUSerwis (integrator systemów dziedzinowych z EZD oraz portalami eusług: eVat, eNależności, eSPrawozdawczość) oraz:
k. SIO Bestia
l. Płatnik

96) Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej co najmniej w pełnym zakresie danych i rejestrów systemów dziedzinowych.

Opracowane dokumentacji powykonawczej

97) Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie obszary będące przedmiotem usługi. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. W szczególności dokumentacja musi zawierać:
    a. Wszelkie zmiany w stosunku do planu wdrożenia z podaniem ich powodów.
    b. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).
    c. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
    d. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.
    e. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.