Załącznik nr 8 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

W ramach zamówienia planowane są dostawy i usługi zgodnie z poniższą specyfikacją.

Lp.	Nazwa urządzenia / usługi	Ilość
1.	Serwer wraz z systemem operacyjnym	1
2.	Macierz dyskowa	1
3.	System archiwizacji danych do serwerów wraz z oprogramowaniem	1
4.	Urządzenie ochrony sieci	1
5.	Zasilacz awaryjny UPS	1
6.	Szafa do serwerowni wraz z osprzętem sieciowym	1
7.	Instalacja i konfiguracja urządzeń	1

Wszystkie dostarczone urządzenia muszą być dostarczone z przewodami umożliwiającymi wpięcie ich do sieci elektrycznej i wykonanie połączeń do sieci logicznej oraz wykonanie połączeń pomiędzy urządzeniami.

Infrastruktura teleinformatyczna

Serwer wraz z systemem operacyjnym

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Maksymalnie 1U RACK 19” (wraz z wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack i umożliwiającymi wysuwanie serwera w celach serwisowych). Obsługa minimum 8 dysków 2.5”.
Płyta główna	Płyta główna dwuprocesorowa - musi być kompatybilna z zainstalowanymi podzespołami. Zaprojektowana i wyprodukowana przez producenta serwera. Fabryczna obsługa pamięci typu SATA DOM o pojemności minimum 128GB. Dwa fabrycznie zainstalowane na płycie głównej sloty na karty SD.
Procesor	Procesor wielordzeniowy wykonany w technologii x86-64 dający wynik min. 275 w teście SPECint_rate2006base dla konfiguracji dwuprocesorowej.
Pamięć RAM	64GB pamięci RAM DDR4 2400MHz z korekcją błędów ECC, SDDC, memory mirroring, memory sparing, lockstep. Moduły pamięci o pojemności minimalnej 16GB. Możliwość instalacji w serwerze min. 1TB pamięci RAM.
Kontroler	Zainstalowany sprzętowy kontroler dyskowy SAS zapewniający obsługę RAID na poziomie minimum 0/1/10. Obsługa dysków SAS 12Gb/s.
Pamięć masowa	Minimum dwa dyski 300GB SAS 10000RPM 12Gb/s. Możliwość instalacji w oferowanym modelu serwera dysków SATA, NL-SAS, SAS, SSD SATA, SSD SAS, NVMe.
Karty sieciowe	2 porty Ethernet minimum 1Gbit RJ45.
Sloty rozszerzeń	Minimum 1 slot PCI-Express 3.0 X16. Możliwość rozbudowy do minimum 2 slotów PCI-Express 3.0 X16. Oferowany serwer musi obsługiwać karty PCI-E oferujące łączność 40Gbit Ethernet oraz InfiniBand FDR 56Gbit. Oferowany serwer musi obsługiwać karty PCI-E SSD o pojemności minimum 3,2TB.
Porty	Minimum 5 portów USB (w tym co najmniej trzy w wersji 3.0), 2 porty VGA, 1 port szeregowy DB9
Karta graficzna	Zintegrowana karta graficzna z płytą główną umożliwiająca wyświetlanie obrazu w rozdzielczości min. 1920x1080 60Hz.
Zasilacze	Minimum 2szt., redundantne typu hot-plug
Zarządzanie i obsługa techniczna	Karta zdalnego zarządzania (konsoli) pozwalająca na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS), zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego. Wymagane dostarczenie funkcjonalność przejęcia zdalnej konsoli graficznej i podłączenia wirtualnych napędów DVD/ISO, współdzielenie konsoli pomiędzy kilku użytkowników. Dostęp z poziomu przeglądarki WWW jak i z linii komend CLI. Dedykowany port zarządzania RJ-45 1Gb/s. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną. Nie dopuszcza się rozwiązań serwerowych wymagających dokupowania dodatkowych licencji umożliwiających zarządzanie serwerem i dostarczających wyżej wymienione funkcjonalności.
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Gwarancja	Minimum 3 lat gwarancji producenta z serwisem świadczonym w miejscu instalacji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

Inne	Serwer musi być wyprodukowany zgodnie z normą ISO 9001 oraz ISO 14001 (dokumenty załączyć do oferty). Serwer musi posiadać deklaracje CE (dokument załączyć do oferty). Firma serwisująca musi posiadać status autoryzowanego partnera serwisowego producenta i posiadać ISO 9001 na świadczenie usług serwisowych – dokumenty potwierdzające załączyć do oferty.
Oprogramowanie	Serwer musi być dostarczony z zainstalowanym systemem operacyjnym. Licencja systemu musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. • Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym; • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny; • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych; • 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; • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy; • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy; • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego; • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; • Wbudowane wsparcie instalacji i pracy na wolumenach, które: – pozwalają na zmianę rozmiaru w czasie pracy systemu, – umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, – umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, – umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość; • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji; • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET; • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów; • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych; • Graficzny interfejs użytkownika; • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);

	• Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu; • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa; • Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management); • 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: – Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, – Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: – Dystrybucję certyfikatów poprzez http, – Konsolidację CA dla wielu lasów domeny, – Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. 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) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, l) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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: – Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, – Obsługi ramek typu jumbo frames dla maszyn wirtualnych, – Obsługi 4-KB sektorów dysków, – Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, – Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie

	kilku innych dostawców poprzez otwarty interfejs API, – Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw trunk mode), • Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet; • Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath); • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego; • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty; • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Macierz dyskowa

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów montażowych.
Kontroler dysków	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active/active. Możliwość rozbudowy do 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączanie kilku macierzy przez wirtualizator zasobów dyskowych). Kontrolery wyposażone w funkcjonalność konfiguracji poziomów RAID: RAID 0, RAID 1 lub RAID10, RAID 5, RAID 6. Zabezpieczenia RAID realizowane za pomocą sprzętowego, dedykowanego układu, z możliwością ich kombinacji w/w typów w ramach oferowanej macierzy. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.
Wewnętrzna pamięć masowa	Fizyczna przestrzeń dyskowa zbudowana za pomocą 6 dysków 2TB NL-SAS 7200RPM. Obsługa dysków SAS 10000RPM o pojemności 1,8TB, dysków SSD SAS o pojemności 1,8TB oraz dysków samoszyfrujących NL-SAS. Macierz musi mieć rozbudowy do co najmniej 500 napędów dyskowych, bez wymiany kontrolerów macierzowych (tylko poprzez dodawanie półek i napędów dysków).
Pamięć	Minimum 16GB pamięci Cache na każdy kontroler. Pamięć Cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci Cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. Możliwość rozbudowy do minimum 128GB pamięci Cache. Rozbudowa nie może odbywać się z udziałem dysków FLASH/SSD.
Interfejsy	Minimum 8 interfejsów 1Gb/s ETH. Możliwość rozbudowy o dodatkowe 32 interfejsy FC 8Gb/s lub 16 interfeisów 1Gb/s ETH.
Prezentacja dysków logicznych	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation).
Zarządzanie	Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii. Zarządzanie macierzą musi odbywać się z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagane dostarczenie w/w funkcjonalność na zainstalowana przestrzeń dyskową.
Replikacja danych	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów

	dyskowych) do macierzy tej samej rodziny w trybie synchronicznym i asynchronicznym. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Na tym etapie postępowania nie jest wymagane dostarczenie w/w funkcjonalności.
Pozostała funkcjonalność	Macierz musi umożliwiać: - ustanawianie polityk dostępu dla użytkowników - migrację LUNów - automatyczną migrację danych na nowododane dyski w celu równego zużycia zasobów dyskowych - multipathing Jeśli wyżej wymienione funkcjonalności wymagają odpowiednich licencji, wymaga się aby te licencje zostały dostarczone z macierzą. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii. Macierz musi mieć możliwość rozbudowy do co najmniej 500 napędów dyskowych, bez wymiany kontrolerów macierzowych (tylko poprzez dodawanie półek i napędów dysków).
Certyfikaty	Macierz musi być wyprodukowana zgodnie z normą ISO 9001 oraz ISO 14001 (dokumenty załączyć do oferty). Macierz musi posiadać deklaracje CE (dokument załączyć do oferty).
Gwarancja	3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

System archiwizacji danych dla serwerów wraz z oprogramowaniem

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	RACK 1U
Pojemność	Dostępna przestrzeń dyskowa 2TB w konfiguracji RAID1
Interfejsy	1 x 1Gbit
Kontroler dysków	Zainstalowany sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów min RAID: 0, 1, 10.
Dostępne złącza	VGA, PS/2, port szeregowy (DB-9)
Backup danych	Rozwiązanie musi zapewnić funkcjonalność scentralizowanego system wykonywania kopii zapasowych w heterogenicznym środowisku (różne systemy operacyjne) z wykorzystaniem następujących protokołów: SMB, CIFS, SSHFS. Rozwiązanie musi wspierać archiwizację danych z systemów Mac OS X. Rozwiązanie ma wspierać archiwizację poczty na poziomie pojedynczej wiadomości z systemów Microsoft Exchange i Novell Gropuwise. Producent zobowiązany jest dostarczyć dedykowanego Agenta do systemów Windows, za pomocą, którego możliwe jest archiwizowanie danych z Microsoft Microsoft SQL, Microsoft Hyper-V, Microsoft Active Directory oraz rejestru systemowego, stanu systemu operacyjnego (ang. System State) i plików przechowywanych na dyskach systemu Microsoft Windows. Agent backupu dostarczany jest dla systemów operacyjnych aktualnie wspieranych przez firmę Microsoft. Agent dla systemów z rodziny Microsoft Windows ma wspierać mechanizm deduplikacji danych. Agent nie wymaga dodatkowej licencji i może być zainstalowany na dowolnej liczbie komputerów. Rozwiązanie ma wspierać archiwizację otwartych i edytowanych plików. Rozwiązanie ma posiadać funkcję automatycznego backupu otwartego I edytowanego pliku. Rozwiązanie ma umożliwiać wykonywanie backapu w oparciu o harmonogram utworzony przez administratora. Rozwiązanie musi umożliwiać definiowanie różnych strategii wykonywania backapu dla poszczególnych obiektów podlegających backupowi.

	Rozwiązanie musi mieć możliwość wykonywania backupu na lokalnie dostarczonym urządzeniu. Rozwiązanie backupowe powinno umożliwiać zarządzanie wieloma urządzeniami tego samego typu przy użyciu jednego interfejsu graficznego. Rozwiązanie musi umożliwiać replikacji danych zapisanych na urządzeniu na zewnętrzne nośniki typu taśmy, VTL, NAS Rozwiązanie musi umożliwiać wykonywanie backup PTV systemów z rodziny Windows na VMware.
Odtwarzanie danych	Odtwarzanie danych musi odbywać się przy użyciu mechanizmów - dedykowanego klienta odtwarzania dla systemów Windows, protokołu FTP, interfejsu WWW, protokołu WebDAV. Dane muszą być odtwarzane przez administratorów urządzenia lub użytkowników końcowych w zależności od uprawnień. Możliwość uruchomienia LiveBoot dla VMWare od wersji 4.0 Możliwość odtworzenia pełnego system operacyjnego zawierającego ustawienia, dane, aplikacje na nowym komputerze.
Raportowanie	Rozwiązanie backupowe powinno udostępniać raporty pozwalające na analizę kluczowych elementów, takich jak: - archiwizowania i odtwarzania danych, - wykorzystania dostępnych zasobów dyskowych i systemowych Rozwiązanie backupowe powinno udostępniać raporty pozwalające na analizę aktywności administratorów i użytkowników. Rozwiązanie backupowe powinno udostępniać pełną historię modyfikacji zarchiwizowanych plików.
Administracja	Rozwiązanie ma być konfigurowane za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową. Rozwiązanie może być zarządzane przez dowolną liczbę administratorów, którzy posiadają rozłączne lub nakładające się uprawnienia. Rozwiązanie powinno posiadać mechanizm informowania administratorów o wystąpieniu błędów za pośrednictwem automatycznie generowanych wiadomości poczty elektronicznej. Rozwiązanie backupowe powinno posiadać opcję informowania w formie wiadomości e-mail o statusie wykonania zadań backupowych na więcej niż jeden adres e-mail.
Certyfikaty	Urządzenie musi posiadać oznakowanie CE.
Gwarancja	Oferowane rozwiązanie musi być objęte 3-letnią gwarancją producenta obejmującą wszystkie elementy rozwiązania wraz z możliwością odpłatnego przedłużenia okresu gwarancji po jej wygaśnięciu na kolejny okres minimum jednego roku. W razie wystąpienia usterki urządzenia, producent w ramach gwarancji przeprowadzi jego wymianę na nowy model. Wysyłka nowego urządzenia następuje w dniu zgłoszenia i potwierdzenia awarii (o ile potwierdzenie nastąpi do godziny 14:00) przez producenta przesyłką kurierską na koszt producenta. Gwarancja musi uwzględniać automatyczne aktualizacje system oraz całodobowe wsparcie techniczne świadczone w języku polskim. Możliwość bezpłatnej wymiany urządzenia na nowe po 48 miesiącach.

Router/Firewall

	Wymagane minimalne parametry techniczne
Informacje ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych

	i programowych systemów zabezpieczeń oraz łączy sieciowych. Dostarczone rozwiązanie musi umożliwić łączenie łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
Funkcje bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych: - Kontrola dostępu – zapora ogniowa klasy Stateful Inspection - Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip. - Poufność danych - IPSec VPN oraz SSL VPN - Ochrona przed atakami - Intrusion Prevention System [IPS/IDS] - Kontrola stron Internetowych – Web Filter [WF] - Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3) - Kontrola pasma oraz ruchu [QoS i Traffic shaping] - Kontrola aplikacji oraz rozpoznawanie ruchu P2P - Analiza ruchu szyfrowanego protokołem SSL
Firewall	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. Musi zapewnić obsługę nie mniej niż 50 tys. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę. Musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Urządzenie ma obsługiwać translacje NAT adresu źródłowego i NAT adresu docelowego. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
VPN	W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: - Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności - Praca w topologii Hub and Spoke oraz Mesh - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth - Obsługa ssl vpn w trybach portal oraz tunel
IPS	Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
Antywirus	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
Web Filter	Baza filtra WWW pogrupowana w min 50 kategorii tematycznych. W ramach filtra www muszą być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
Kontrola aplikacji	Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
Porty	System musi dysponować minimum 5 interfejsami miedzianymi Ethernet 10/100/1000.
Interfejsy wirtualne	Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.

Obsługa połączeń	W zakresie Firewall'a obsługa nie mniej niż 50 tys jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.
Obsługa Routingu	Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
Uwierzytelnianie	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych ; - Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny;
Wydajność	Wydajność systemu Firewall min 500 Mbps. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 150 Mbps. Wydajność ochrony przed atakami (IPS) min 500 Mbps. Wydajność VPN IPSec, nie mniej niż 250 Mbps.
Raportowanie	System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż: - Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego - Generowanie co najmniej 25 różnych typów raportów System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania.
Polityka bezpieczeństwa	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
Aktualizacja	Wymagane jest automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
Zarządzanie	Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Certyfikaty	Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ dla rozwiązań kategorii Network Firewall.
Gwarancja	3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Licencje dla wszystkich funkcji bezpieczeństwa na okres minimum 36 m-ce liczoną od dnia zakończenia wdrożenia całego systemu.

Zasilacz awaryjny

Nazwa komponentu	Wymagane minimalne parametry techniczne
Moc wyjściowa pozorna / czynna	3000 VA / 1950 W
Typ obudowy	RACK
Znamionowe napięcie wejściowe	230 V
Częstotliwość znamionowa	50 Hz

napięcia wejściowego	
Zakres napięcia wyjściowego	230V ±10%
Czas podtrzymania z baterii wewnętrznych	15 min przy 50% obciążenia maksymalnego
Zabezpieczenie wejściowe	Przeciwzwarciowe i przeciwprzepięciowe
Zabezpieczenie wyjściowe	przeciwzwarciowe i przeciążeniowe
Gniazda przyłącza wyjściowego	5 x IEC 320 C13
Inne	Zimny start. Przewód zasilający zakończony wtyczką z uziemieniem. Filtr telekomunikacyjny. Dźwiękowa sygnalizacja rozładowania baterii.
Gwarancja	3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

Szafa do serwerowni wraz z osprzętem sieciowym

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Szafa serwerowa typu RACK 42 U o wymiarach 800mm x 1000mm. na cokole z płytą dolną otworowaną umożliwiającą doprowadzenie okablowania. Drzwi szafy powinny być perforowane w celu umożliwienia właściwego przepływu chłodnego powietrza.
Wyposażenie	Szafa musi być wyposażona w panel 4 wentylatorów, minimum jedną listwę zasilającą 16A z minimum 6 gniazdami w obudowie aluminiowej, wyposażoną w filtr przeciwzakłóceniowy, panele porządkujące oraz zestaw śrub umożliwiających montaż urządzeń w szafie.
Gwarancja	3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

Instalacja i konfiguracja

Nazwa komponentu	Wymagane minimalne parametry techniczne
Instalacja i konfiguracja	Zamawiający wymagana instalację wszystkich dostarczonych urządzeń, podpięcie ich do istniejącej sieci elektrycznej i infrastruktury logicznej sieci LAN oraz jeżeli jest to konieczne wykonanie połączeń pomiędzy urządzeniami. Oprogramowanie systemowe dostarczone wraz z serwerem musi być zainstalowane i skonfigurowane w sposób umożliwiający pracę całego systemu. Macierz dyskowa musi być przygotowana do pracy, musi mieć skonfigurowane dyski w układzie RAID, a przestrzeń dyskowa musi być podzielona wolumeny. Macierz musi udostępniać zasoby dla serwera. System archiwizacji musi być skonfigurowany zgodnie z wytycznymi administratora Zamawiającego, w sposób umożliwiający na automatyczne tworzenie kopii bezpieczeństwa. Urządzenie ochrony sieci musi mieć skonfigurowane wszystkie systemy dostarczone w ramach rozwiązania (firewall, IPS, NAT, routing, itp). Zamawiający wymaga przeprowadzenia testów weryfikujących poprawność konfiguracji.