*Załącznik nr 7 do SIWZ*

**OPIS PRZEDMIOTU ZAMÓWIENIA**

I. **ZAKRES DOSTAW I USŁUG**

Niniejsze zamówienie dotyczy dostaw sprzętu informatycznego wraz z realizacją usług instalacyjno konfiguracyjnych, zgodnie z poniższym zestawieniem. Oferowane rozwiązania muszą spełniać minimalne wymagania zawarte w niniejszej specyfikacji.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Lp.** |  | **Nazwa urządzenia / usługi** |  | **Ilość** |
| 1. | | Serwer wraz z systemem operacyjnym | | 1 | |
| 2. | | System archiwizacji danych | | 1 | |
| 3. | | Urządzenie ochrony sieci | | 1 | |
| 4. | | Przełącznik sieciowy | | 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.

II. **RÓWNOWAŻNOŚĆ ROZWIĄZAŃ**

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym.

W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

Mając na uwadze powyższe Zamawiający informuje, że w sytuacji, gdy Wykonawca w złożonej ofercie przetargowej nie wykaże, iż proponowane materiały i urządzenia zamienne, inne niż określone w dokumentacji projektowej, są równoważne pod względem konstrukcji, parametrów technicznych,

jakościowych i funkcjonalnych oraz ich przeznaczenia, spowoduje to uznanie przez Zamawiającego, że złożona oferta nie odpowiada treści SIWZ w zakresie opisu przedmiotu zamówienia i zostanie z niniejszego postępowania przetargowego odrzucona.

Jeśli w opisach niniejszego OPZ występują: normy, europejskie oceny techniczne, aprobaty, specyfikacje techniczne lub systemy referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3 ustawy PZP należy to traktować jedynie, jako pomoc w opisie przedmiotu zamówienia. W każdym przypadku dopuszczalne są rozwiązania równoważne opisywanym.

III. **GWARANCJA**

Dla wszystkich urządzeń Zamawiający wymaga 3 letniego okresu gwarancji, z serwisem realizowanym w miejscu instalacji sprzętu oraz z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia i możliwością zgłaszania awarii poprzez linię telefoniczną producenta lub autoryzowanej firmy serwisującej.

Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu

zamówienia.

Gwarancja musi uwzględniać:

a) pozostawienie uszkodzonych dysków twardych u Zamawiającego w przypadku jego wymiany –

dotyczy serwera;

b) aktualizacje, w okresie obowiązywania gwarancji, subskrypcji wszystkich funkcji bezpieczeństwa wymaganych dla urządzenia ochrony sieci.

Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.

IV.**MINIMALNE WYMAGANIA**

1. **Serwer typu RACK**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **OBUDOWA** | Maksymalnie 2U 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” z możliwością obsługi napędów LTO lub rozbudowy do 28 dysków 2.5”. |
| **PŁYTA GŁÓWNA** | Płyta główna z możliwością zainstalowania do dwóch procesorów oraz możliwością obsługi min. 12 slotów pamięci na każdy procesor.  Obsługa nośników dla wirtualizatora. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde jak i portów USB oraz slotów PCIe |
| **PROCESOR** | Zainstalowany min 12 rdzeniowy 24 wątkowy, z najnowszej dostępnej na rynku generacji procesorów. |

|  |  |
| --- | --- |
| **PAMIĘĆ RAM** | Minimum 32GB pamięci RAM typu RDIMM 2400MT/s z możliwością rozbudowy  do 1,5TB  Zabezpieczenia pamięci: Memory Mirror, Memory Sparing. |
| **KONTROLER DYSKOWY** | Zainstalowany sprzętowy kontroler dyskowy. Możliwe konfiguracje poziomów  RAID: 0, 1, 5, 6, 10, 50, 60. Posiadający minimum 1GB nieulotnej pamięci Cache. |
| **PAMIĘĆ MASOWA** | Minimum dwa dyski 1,2TB SAS 15k RPM 12Gb/s HotPlug.  Możliwość instalacji w oferowanym modelu serwera dysków SATA, NL-SAS, SAS, SSD SATA, SSD SAS, NVMe.  Możliwość instalacji na płycie głównej modułu pamięci półprzewodnikowej min  16GB dedykowany do instalacji hypervisora ESXi o trwałości określonej  parametrem MTBF nie mniejszym niż 8 mln. godzin. |
| **KARTY SIECIOWE** | Minimum dwie niezależne karty sieciowe posiadające po min dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  Interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express oraz portów USB. Wsparcie dla protokołów iSCSI Boot oraz IPv6.  Zamawiający wymaga dostarczenia kabli RJ45 3m dla każdego wbudowanego  interfejsu sieciowego. |
| **SLOTY ROZSZERZEŃ** | Minimum 8 złącz PCI Express generacji 3 low profile, w tym minimum 3 złącza o prędkości x16 |
| **PORTY** | Minimum 5 portów USB (w tym co najmniej pięć w wersji 3.0), 2 porty VGA, 1 port szeregowy RS232 |
| **KARTA GRAFICZNA** | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |
| **ZASILACZE** | Redundantne zasilacze Hot Plug o mocy dopasowanej do samodzielnego zapewnienia zasilania dla całego serwera oraz sprawności min 96%.  Każdy zasilacz musi być dostarczony wraz z kablami zasilającymi o dł. min. 1,5m. |
| **ZARZĄDZANIE I OBSŁUGA**  **TECHNICZNA** | Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden port  10/100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł musi umożliwiać:  - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika  - podmontowanie zdalnych wirtualnych napędów,  - dostęp do myszy, klawiatury z wykorzystaniem wirtualnej konsoli,  - przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym  - karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze  - wsparcie dla IPv6,  - wysyłanie do administratora maila z powiadomieniem o awarii lub  zmianie konfiguracji sprzętowej,  - wsparcie dla protokołu SNMP,  - wsparcie DNS i usług katalogowych,  - możliwość zarządzania poborem prądu,  Oprogramowanie do zdalnego zarządzania serwerem musi umożliwiać: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za |

str. 4

|  |  |
| --- | --- |
|  | pomocą sygnalizatora optycznego, wysyłanie zawiadomień droga mailową lub poprzez SNMP, niezależnie od zainstalowanego systemu operacyjnego  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. |
| **CERTYFIKATY** | Wymagane oznaczenie produktu znakiem CE lub równoważnym.  Oferowany serwer musi znajdować się na liście kompatybilności producenta  systemu operacyjnego dostarczonego wraz z serwerem.  W przypadku braku w/w certyfikatów na internetowych stronach producenta, Zamawiający na etapie weryfikacji oferty będzie wymagał przedstawienia dokumentów potwierdzających spełnienie przez produkt w/w wymagań jakościowych. |
| **OPROGRAMOWANIE** | Serwer musi być dostarczony z zainstalowanym systemem operacyjnym. Licencja  systemu musi być przypisana do każdego procesora fizycznego i musi  uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze.  Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Musi zapewnić wsparcie (na umożliwiającym to sprzęcie) dodawania pamięci RAM  bez przerywania pracy.  Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.  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 uruchamiania aplikacji internetowych  wykorzystujących technologię [ASP.NET.](http://asp.net/)  Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów .  Wbudowana zapora internetowa (firewall) z obsługi 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.  Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.  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). |

str. 5

Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

- Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

- Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie ui:ytkownik6w stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarzadzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

podłączenie 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.

Zdalna dystrybucja oprogramowania na stacje robocze.

Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

PKI (Centrum Certyfikat6w (CA), obsługa klucza publicznego i prywatnego)

umożliwiające:

- dystrybucję certyfikatów poprzez http,

- konsolidację CA dla wielu lasów domeny,

- automatyczne rejestrowania certyfikat6w pomiędzy różnymi lasami domen. Szyfrowanie plików i folderów.

Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami

roboczymi (IPSec).

Serwis udostępniania stron [WWW.](http://www/) Wsparcie dla protokołu IP w wersji 6 (IPv6).

Wbudowane usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

**2. System archiwizacji danych**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **INFORMACJE OGÓLNE** | System backup-u danych musi realizować wszystkie poniższe funkcjonalności. Rozwiązanie musi umożliwiać tworzenie kopii zapasowych na dyskach twardych  zapewniających wysoką dostępność poprzez przechowywanie danych na macierzy  RAID, minimum na jednym z poziomów: RAID1, RAID10 lub RAID 5.  Dostępna przestrzeń do przechowywania kopii zapasowych nie może być mniejsza jak  2TB.  Dopuszcza się, aby elementy wchodzące w skład systemu backup 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. |
| **OBUDOWA** | Obudowa typu RACK 19” o wysokości maksymalnie 2U |
| **POJEMNOŚĆ** | Dostępna przestrzeń dyskowa 2TB w konfiguracji RAID1 |

str. 6

|  |  |
| --- | --- |
| **INTERFEJSY** | Minimum 1 interfejs sieciowy 1 Gigabit.  Dostępne złącza:  - minimum 1 x VGA;  - minimum 2 porty USB. |
| **ADMINISTRACJA** | Rozwiązanie ma być konfigurowane za pomocą graficznego interfejsu.  Rozwiązanie może być zarządzane przez dowolną liczbę administratorów, którzy posiadają rozłączne lub nakładające się uprawnienia.  Rozwiązanie musi posiadać mechanizm informowania administratorów o wystąpieniu błędów za pośrednictwem automatycznie generowanych wiadomości poczty elektronicznej.  Rozwiązanie backupowe musi posiadać opcję informowania w formie wiadomości e- mail o statusie wykonania zadań backupowych na więcej niż jeden adres e-mail. Rozwiązanie musi zapewniać możliwość pełnego centralnego zarządzania przez www modułem wykonywania kopii zapasowych na serwerach w zakresie:  konfiguracji parametrów wykonywania kopii zapasowych,  przydzielania zadań wykonywania kopii zapasowych,  monitorowania stanu wykonania kopii zapasowych,  powiadamiania o stanie zadań backupu drogą mailową,  przeglądania i odtwarzania wybranych elementów wykonanych kopii  zapasowych,  monitorowania w trybie graficznym aktualnego stanu systemu z uwzględnieniem:  statusu wykonanych zadań backupu (udane/nieudane),  aktualnej wielkości danych backupowych,  aktualnej zajętości repozytorium backupu,  trendów objętości backupu,  wielkości danych w repozytoriach backupu z uwzględnieniem rzeczywistej wielkości danych źródłowych i objętości z uwzględnieniem kompresji i deduplikacji. |
| **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. |

str. 7

|  |  |
| --- | --- |
|  | 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. |
| **CERTYFIKATY** | Urządzenie musi posiadać deklarację CE lub równoważną.  W przypadku braku w/w certyfikatów na internetowych stronach producenta, Wykonawca będzie musiał dołożyć dokumenty potwierdzające spełnienie przez produkt wymagań jakościowych. |

**3. Urządzenie ochrony sieci**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **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, |

str. 8

|  |  |
| --- | --- |
|  | 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 100 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; |

str. 9

|  |  |
| --- | --- |
|  | - 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 2 Gbps.  Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall,  Antivirus min. 250 Mbps.  Wydajność ochrony przed atakami (IPS) min 1,5 Gbps.  Wydajność VPN IPSec, nie mniej niż 300 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. |

**4. Przełącznik sieciowy**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **OBUDOWA** | Obudowa typu RACK 19”; Wysokość maksymalna 1U;  Wewnętrzny zasilacz 230V AC o mocy dopasowanej do samodzielnego zapewnienia  zasilania urządzenia; |
| **PORTY** | 48 x 10/100/1000Base-T;  2 x SFP  2 x 10G SFP+; |
| **WYDAJNOŚĆ** | Matryca przełączająca o wydajności min. 140 Gbps;  Wydajność przełączania przynajmniej 100 Mpps; |
| **BEZPIECZEŃSTWO** | Autoryzacja użytkowników w oparciu o IEEE 802.1x |
| **ZARZĄDZANIE** | ACL - Access Control List  SSH SSH2  SSL |
| **INNE** | Urządzenie musi być zamontowane w szafie RACK i uruchomione. |

str. 10

|  |  |
| --- | --- |
|  | Porty Base-T muszą być połączone za pomocą kabli krosowych z odpowiednimi  gniazdami RJ45 w panelach krosowych sieci LAN.  Urządzenie musi być skonfigurowane zgodnie ze wskazaniami i uzgodnieniami z Zamawiającym na etapie instalacji. |
| **CERTYFIKATY** | Urządzenie musi posiadać oznakowanie CE lub równoważne.  W przypadku braku w/w deklaracji na internetowych stronach producenta, Zamawiający na etapie weryfikacji oferty będzie wymagał przedstawienia dokumentów potwierdzających spełnienie przez produkt w/w wymagań jakościowych. |

**5. Zasilacz awaryjny**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Nazwa komponentu** |  | **Wymagane minimalne parametry techniczne** |
| **TYP OBUDOWY** | | Obudowa typu RACK, wysokość maksymalna 2U | |
| **RODZAJ ZASILACZA** | | On-line | |
| **MOC WYJŚCIOWA POZORNA / CZYNNA** | | 3000 VA / 2700 W | |
| **ZNAMIONOWE NAPIĘCIE WEJŚCIOWE** | | 230 V | |
| **CZĘSTOTLIWOŚĆ ZNAMIONOWA NAPIĘCIA WEJŚCIOWEGO** | | 50 Hz | |
| **ZAKRES NAPIĘCIA WYJŚCIOWEGO** | | 230V ±10% | |
| **CZAS PODTRZYMANIA Z BATERII**  **WEWNĘTRZNYCH** | | Minimum 11 min przy 50% obciążenia maksymalnego | |
| **ZABEZPIECZENIE WEJŚCIOWE** | | Przeciwzwarciowe i przeciwprzepięciowe | |
| **ZABEZPIECZENIE WYJŚCIOWE** | | przeciwzwarciowe i przeciążeniowe | |
| **GNIAZDA PRZYŁĄCZA WYJŚCIOWEGO** | | Min 8 x IEC320 C13 oraz min 2x IEC 320 C19 | |
| **PORTY** | | Minimum: 1 x USB, 1xRJ45 (SNMP) | |
| **INNE** | | Wielofunkcyjny wyświetlacz LCD  Oprogramowanie zarządzająco-monitorujące ze wsparciem dla ESXi  Możliwość zwiększenia czasu podtrzymania zasilania przez rozszerzenie o kolejne moduły bateryjne  Zimny start.  Przewód zasilający zakończony wtyczką z uziemieniem.  Filtr telekomunikacyjny.  Dźwiękowa sygnalizacja rozładowania baterii.  Pakiet serwisowy musi obejmować zarówno sam UPS jak i baterie akumulatorów na cały okres gwarancji | |

**6. Szafa serwerowa typu RACK**

|  |  |
| --- | --- |
| **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. |

str. 11

|  |  |
| --- | --- |
| **DRZWI** | Drzwi przednie szafy, zamykane na zamek, perforowane w celu  umożliwienia właściwego przepływu chłodnego powietrza.  Drzwi tylne stalowe uchylne z zamkiem.  Drzwi boczne demontowane na zatrzaskach z możliwością montażu zamka. |
| **WYPOSAŻENIE** | Panel wentylacyjny z 4 wentylatorami.  Minimum trzy półki.  Minimum jedna listwa zasilająca 16A z minimum 6 gniazdami w obudowie  aluminiowej, wyposażoną w filtr przeciwzakłóceniowy.  Panele porządkujące oraz zestaw śrub umożliwiających montaż urządzeń w  szafie. |

**7. 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.  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. |

str. 12