**Załącznik nr 7 do SIWZ**

**SPECYFIKACJA ASORTYMENTOWA**

1. **Szafa rack – Producent …………………. / model ………………………**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SZAFA RACK** | | | **Ilość** | **1 sztuka** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | | |
| **Wymiary** | 42U 19" 600 x 1000 mm (szer. x gł.) |  | | |
| **Typ** | Stojąca, skręcana |  | | |
| **Drzwi** | Perforowane |  | | |
| **Obciążenie** | Min. 800kg |  | | |
| **Otwory kablowe** | Góra, dół |  | | |
| **Otwór na wentylator** | Tak |  | | |
| **Klasa szczelności** | IP20 |  | | |
| **Osprzęt montażowy** | * Komplet śrub, * panel wentylacyjny podwójny z termostatem elektronicznym, * cokół. |  | | |
| **Gwarancja** | 24 miesiące |  | | |

1. **Przełącznik KVM z KMM – Producent …………………. / model ………………………**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRZEŁĄCZNIK KVM z KMM** | | **Ilość** | **1 sztuka** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| **Liczba portów** | Obsługa 8 komputerów jedną konsolą |  | |
| **obudowa** | Rack 1U, Zintegrowana konsola KVM z 19-calowym monitorem |  | |
| **Urządzenia wskazujące** | Klawiatura i touchpad |  | |
| **Funkcje** | * Podwójny interfejs – obsługuje komputery z klawiaturą i myszą PS/2 lub USB, * Automatyczne wykrywanie interfejsów PS/2 i USB, * Emulacja klawiatury i myszy USB lub PS/2 – komputery uruchamiają się nawet wtedy, gdy konsola zajmuje się innymi zadaniami, * Jakość wideo – do 1280 x 1024 @ 75 Hz, * Wygodne przełączanie komputerów za pomocą przycisków na panelu czołowym lub za pomocą menu ekranowego w wielu językach, * Dwupoziomowe zabezpieczenie hasłem – tylko autoryzowani użytkownicy widzą i kontrolują komputery; do czterech użytkowników i jeden administrator, każdy  z oddzielnym profilem, * Funkcja autoskanowania do monitorowania komputera wybranego przez użytkownika, * Tryb rozgłaszania – jednoczesne wykonywanie operacji na wszystkich wybranych komputerach, * Możliwość podłączania w trakcie pracy – podłączanie lub odłączanie komputerów bez odłączania zasilania. |  | |
| **Akcesoria** | Dołączone 8 kabli KVM USB |  | |
| **Gwarancja** | 24 miesiące |  | |

1. **SSWiN+KD – Producent ……………../ model …………………..**

|  |  |  |  |
| --- | --- | --- | --- |
| **SSWiN+KD** | | **Ilość** | **1 komplet** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| Elementy wyposażenia systemów SSWiN oraz KD | * + - * Centrala systemu SSWiN wraz z dedykowanym modułem KD  z wbudowanym komunikatorem GSM/GPRS z funkcjami monitoringu, powiadamiania i zdalnego sterowania – 1 komplet,       * Moduł komunikacji TCP/IP -1 sztuka,       * Manipulator systemu alarmowego z czytnikiem kart – 1 sztuka,       * Przycisk wyjścia natynkowy – 1 sztuka,       * Przycisk awaryjnego otwierania drzwi – 1 sztuka,       * Zwora elektromagnetyczna z czujnikiem stanu drzwi – 1 sztuka,       * Cyfrowa pasywna czujka podczerwieni – 2 sztuki,       * Programowalna czujka temperatury – 2 sztuki, * Czujka zalania wodą – 4 sztuki, * Czujka dymu i ciepła – 2 sztuki – zamontowane wewnątrz i na zewnątrz szafy serwerowej, * Zewnętrzny sygnalizator optyczno-akustyczny – 1 sztuka, * Wewnętrzny sygnalizator optyczno-akustyczny – 1 sztuka, * Obudowa z wyposażeniem – 1 komplet, * Karty dostępu – 10 sztuk. |  | |
| **Instalacja** | Wykonawca zainstaluje, podłączy, uruchomi i skonfiguruje system SSWiN+KD w pomieszczeniu Serwerowni,  Po uruchomieniu przeszkoli dział Informatyki z konfiguracji i obsługi. |  | |
| **Gwarancja** | 24 miesiące |  | |

1. **Klimatyzacja – Producent ………………./ model …………………..**

|  |  |  |
| --- | --- | --- |
| **System klimatyzacji** | **Ilość** | **1 sztuka** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** |
| Układ pracy klimatyzatorów | 1 nowy spełniający poniższe wymagania, jako zapasowy pozostawiony istniejący klimatyzator uruchamiany ręcznie |  |
| Moc chłodnicza klimatyzatora | 6,8 kW |  |
| Funkcje | * Automatyczne wybranie trybu chłodzenia lub grzania w celu osiągnięcia ustawionej temperatury, * Możliwość wyboru automatycznego ruchu klap nawiewu w pionie, zapewniający skuteczne rozprowadzenie powietrza i temperatury w całym pomieszczeniu, * Klimatyzator może działać jako wentylator, nawiewając powietrze bez chłodzenia lub grzania, * Program umożliwiający zmniejszenie poziomu wilgotności powietrza bez wahań temperatury w pomieszczeniu, * Automatyczne uruchomienie po zaniku napięcia. |  |
| Autodiagnostyka | * Informacja o stanie urządzeń, * identyfikacja nieprawidłowości w pracy urządzeń, |  |
| Wymagania | * System klimatyzacji musi zapewnić wymagane warunki temperatury w pomieszczeniu na poziomie 22 stopni C +/-2 stopnie chłodzenia w zakresie temperatur od -15⁰C do +35⁰C |  |
| Gwarancja | 5 lat bezpłatne przeglądy gwarancyjne dla nowego klimatyzatora (co najmniej 2 razy na rok) |  |

1. **Zasilacz** **UPS – Producent ……………… / model …………….**

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS – TYP B** | | **Ilość** | **6 sztuk** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| Moc pozorna | 1000VA |  | |
| Moc czynna | 650W |  | |
| Napięcie wejściowe | 230V |  | |
| Topologia | VI (line interactive) |  | |
| Typ obudowy | Rack 19”, max 2U, głębokość max. 250mm |  | |
| Automatyczna regulacja napięcia (AVR) | Wymagane |  | |
| Filtracja napięcia wyjściowego | Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy |  | |
| Czas przełączenia na pracę rezerwową | < 3 ms |  | |
| Przeciążalność | > 105% - 3 s (wyłączenie UPS – praca bateryjna)  >120% (wyłączenie UPS – praca bateryjna) |  | |
| Czas podtrzymania z baterii wewnętrznych  (100 % / 80 % / 50 % Pmax) | 3 / 4 / 8 min |  | |
| Zabezpieczenie wejściowe | Przeciwzwarciowe  Przeciwprzepięciowe |  | |
| Zabezpieczenie wyjściowe | Elektroniczne – przeciwzwarciowe i przeciążeniowe |  | |
| Przyłącze zasilania UPS | Przewód zakończony wtyczką z uziemieniem 16A |  | |
| Przyłącza wyjściowe (liczba i typ gniazd) | 3 x IEC320 C13 (10 A) oraz 2 x PN-E-93201 |  | |
| Gwarancja | 24 miesiące UPS oraz 24 miesiące akumulatory |  | |

1. **Modernizacja sieci LAN – sieć FO i WiFi – Producent okablowania …………………**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** |
| **Sieć FO** | Parametry kabla światłowodowego:  Kat. kabla wg ISO11801 ed.2.2 OS2  Powłoka zewnętrzna Uniwersalna  Budowa kabla Luźna tuba  Taśma absorbująca wilgoć tak  Ochrona przeciw gryzoniom tak  Wzmocnienie kabla Włókno szklane  Klasyfikacja ogniowa powłoki zew. LSZH  Standardy klasyfikacji ogniowej:   * IEC 60332-1 test na rozchodzenie się ognia * IEC 60754-2 test na stopień kwasowości gazów * IEC 61034 test na gęstość zadymienia   lub równoważne |  |
| **Sieć WiFi** | Parametry kabla miedzianego:   * Zgodność z normami: IEC 11801, EN 50173-1, Kat.6A zgodnie z IEC 61156-5, EN 50288-10-1 * Budowa przewodu: 4 indywidualnie ekranowane zwinięte pary * Izolacja: Bezhalogenowy materiał komórkowy * Ekran na parze: Laminowana folia aluminiowa * Ekran ogólny: Laminowana folia aluminiowa * Płaszcz ochronny: LS0H, FRNC zgodnie z:   o IEC 61034, EN 50268  o IEC 60754, EN 50267  o IEC 60332-1, EN 60332-1 |  |
| **Gwarancja na system okablowania strukturalnego** | 25 lat – wymagana certyfikacja |  |

1. **Zabezpieczenie styku z Internetem – Producent ………………… / model ……………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FIREWALL - UTM** | | **Ilość** | | **1 sztuka** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | | **Oferowane parametry** | |
| **OBSŁUGA SIECI** | * Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP. | |  | |
| **ZAPORA KORPORACYJNA (Firewall)** | * Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection, * Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT, * Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge), * Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie, * Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia, * Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u. * Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów), * Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy  z uwierzytelnieniem Windows 2k (Kerberos). | |  | |
| **INTRUSION PREVENTION SYSTEM (IPS)** | * System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe, * Moduł IPS musi być opracowany przez producenta urządzenia.  Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy, * Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków  i zagrożeń, * Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. * Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej, * Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS, * Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. | |  | |
| **KSZTAŁTOWANIE PASMA (Traffic Shapping)** | * Urządzenie ma mieć możliwość kształtowania pasma w oparciu  o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma, * Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP, * Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring), * Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. | |  | |
| **OCHRONA ANTYWIRUSOWA** | * Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania), * Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji, * Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym, * Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. | |  | |
| **OCHRONA ANTYSPAM** | * Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). * Ochrona antyspam ma działać w oparciu o:   + białe/czarne listy,   + DNS RBL,   + heurystyczny skaner. * W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL, * Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być  w formacie zgodnym z formatem programu Spamassassin. | |  | |
| **WIRTUALNE SIECI PRYWANTE (VPN)** | * Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja), * Odpowiednio kanały VPN można budować w oparciu o:   + PPTP VPN,   + IPSec VPN,   + SSL VPN. * SSL VPN musi działać w trybach Tunel i Portal, * W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem, * Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover), * Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf, * Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. | |  | |
| **FILTR DOSTĘPU DO STRON WWW** | * Urządzenie ma posiadać wbudowany filtr URL, * Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych, * Administrator musi mieć możliwość dodawania własnych kategorii URL, * Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora, * Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny  z protokołem ICAP co najmniej w trybie REQUEST, * Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:   + blokowanie dostępu do adresu URL,   + zezwolenie na dostęp do adresu URL,   + blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. * Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony, * Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych, * Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS, * Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME, * Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane, * Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. | |  | |
| **UWIERZYTELNIANIE** | * Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:   + lokalną bazę użytkowników (wewnętrzny LDAP),   + zewnętrzną bazę użytkowników (zewnętrzny LDAP),   + usługę katalogową Microsoft Active Directory. * Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP, * Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:   + SSL,   + Radius,   + Kerberos. * Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory, * Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta, * Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. | |  | |
| **ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)** | * Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing), * Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:   + równoważenie względem adresu źródłowego,   + równoważenie względem połączenia. * Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu, * Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. * Urządzenie ma posiadać mechanizm statycznego trasowania pakietów, * Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego, * Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP, * Rozwiązanie powinno zapewniać obsługę routingu dynamiczny  w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP, * Rozwiązanie powinno wspierać technologię Link Aggregation. | |  | |
| **POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA** | * Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci, * Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay, * Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4  i IPv6, * Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS, * Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3, * Urządzenie musi posiadać usługę DNS Proxy. | |  | |
| **ADMINISTRACJA URZĄDZENIEM** | * Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia, * Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego, * Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową, a komunikacja musi być zabezpieczona za pomocą protokołu https, * Komunikacja może odbywać się na porcie innym niż https (443 TCP), * Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami, * Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana, * Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https, * Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS), * Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX, * Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora, * Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. | |  | |
| **RAPORTOWANIE** | * Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. * System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania, * System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego  i Antyspamowego, * System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów, * System raportujący ma dawać możliwość edycji konfiguracji  z poziomu raportu, * W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów  i tworzenia raportów w postaci wirtualnej maszyny, * Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy | |  | |
| **PARAMETRY SPRZĘTOWE** | * Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 320 GB, * Liczba portów Ethernet 10/100/1000Mbps – min. 8, * Urządzenie musi pozwalać na podłączenie minimum jednej karty rozszerzeń z 8 interfejsami Ethernet 10/100/1000Mbps lub 4 światłowodowymi interfejsami 1Gbps lub 2 światłowodowymi interfejsami 10Gbps. Urządzenie musi być dostarczone z modułem  z 2 portami światłowodowymi z interfejsami 10Gbps. Dodatkowo należy dostarczyć transceiver światłowodowy o prędkości 10Gbps kompatybilny z urządzeniem oraz transceiver światłowodowy  o prędkości 10Gbps kompatybilny z przełącznikiem sieciowym, * Urządzenie musi posiadać funkcjonalność budowania połączeń  z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta, * Przepustowość Firewalla – min. 10 Gbps, * Przepustowość Firewalla wraz z włączonym systemem IPS – min. 7 Gbps, * Przepustowość filtrowania Antywirusowego – min. 1,6 Gbps, * Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 2 Gbps, * Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000, * Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150, * Obsługa min. VLAN 256, * Liczba równoczesnych sesji - min. 1 000 000 i nie mniej niż 40 000 nowych sesji/sekundę, * Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive, * Urządzenie jest nielimitowane na użytkowników. | |  | |
| **Wymagane licencje / gwarancja** | Urządzenia mają być objęte min. 36 miesięczną gwarancją typu NBD tzn.  w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii.  Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku.  Urządzenie mają posiadać wykupioną licencję na w/w funkcjonalności na okres 36 miesięcy.  Wykonawca musi dostarczyć urządzanie z polskojęzyczną dokumentacją/instrukcję. | |  | |

1. **UPS typ A - dla potrzeb serwerów – Producent ………………. / model …………..**

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS – TYP A** | | **Ilość** | **6 sztuk** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| Moc pozorna | 1500VA |  | |
| Moc czynna | 1350W |  | |
| Napięcie wejściowe | 230V |  | |
| Zakres napięcia wejściowego | 160/140/120/110V – 300V dla obciążenia 100-80%/80-70%/70-60%/60-0% |  | |
| Częstotliwość wejściowa | 45-55Hz lub 56-65Hz |  | |
| Wejściowy współczynnik mocy | 0,99 (nominalne napięcie, pełne obciążenie) |  | |
| Napięcie wyjściowe | 208V, 220V, 230V, 240V |  | |
| Tolerancja napięcia wyjściowego | ±1% |  | |
| Częstotliwość wyjściowa | 50/60Hz ±0,1% |  | |
| Czas przełączania | 0 ms |  | |
| Tryb pracy | true on-line |  | |
| Kształt napięcia wyjściowego | Czysta sinusoida |  | |
| Zniekształcenia napięcia wyjściowego | ≤2% THD przy liniowym obciążeniu  ≤4% THD przy nieliniowym obciążeniu |  | |
| Współczynnik szczytu | 3:1 |  | |
| Gniazda wyjściowe | 8 x IEC 320 (10A) |  | |
| Komunikacja | port RS 232, USB, karta sieciowa SNMP |  | |
| Zdalne wyłączenie | złącze EPO (ppoż.) |  | |
| Poziom hałasu | < 50dB(A) / 1m |  | |
| Baterie | Szczelne, bezobsługowe, ołowiowo-kwasowe |  | |
| Czas ładowania do 90% | 4 godziny |  | |
| Prąd ładowania | 1,5A (max.) |  | |
| Wykonanie | Wersja RACK, mocowanie do szafy rack w zestawie |  | |
| Czas podtrzymania | 5 minut |  | |
| Wymiary UPS (szer x gł x wys) | UPS - 438 x 410 x 88 [2U] mm; |  | |
| Sprawność | 91% - tryb AC-AC  90% - tryb baterii  97% - tryb ECO |  | |
| Dodatkowe cechy zasilacza | * wyświetlacz LCD, * sterowanie mikroprocesorowe, * funkcja Cold Start – załączanie obciążonego urządzenia bez napięcia w sieci, * system automatycznego ładowania baterii * podział gniazd wyjściowych na zarządzalne grupy, * ochrona przepięciowa linii tel/fax/modem, * możliwość pracy jako konwerter częstotliwości z 50Hz na 60Hz lub z 60Hz na 50Hz, * współpraca z agregatami prądotwórczymi, * opcjonalna możliwość zdalnego włączania  i wyłączania zasilacza UPS bez użycia dodatkowego oprogramowania, karty sieciowej SNMP oraz karty styków bezpotencjałowych, * opcjonalna możliwość monitorowania w trybie on-line pracy każdego akumulatora z osobna, pomiar napięcia na każdym z akumulatorów oraz skuteczne ostrzeganie o wykrytych problemach w badanych akumulatorach, * zwiększone bezpieczeństwo podczas transportu (użycie złącza ANNEN), * zabezpieczenie przed głębokim rozładowaniem baterii akumulatorów. |  | |
| Wskaźniki ostrzeżenia na wyświetlaczu LCD | * niski poziom baterii, * przeciążenie, * akumulator nie jest podłączony, * przeładowanie baterii, * błędne podłączenie kabli zasilających, * aktywacja EPO, * przegrzanie, * awaria ładowarki, * awaria baterii, * wyjście poza zakres napięcia linii bypassu, * niestabilna częstotliwość linii bypassu, * błąd EEPROM, * awaria wentylatora, * wymiana baterii. |  | |
| Gwarancja | 1. miesiące UPS oraz 24 miesiące akumulatory |  | |

1. **Przełącznik serwerowy – Producent …………………… / model ………………………**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRZEŁĄCZNIK SERWEROWY** | | **Ilość** | **2 sztuki** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| **Obudowa** | Umożliwiająca montaż w szafie rack 19” |  | |
| **Liczba gniazd** | wbudowane 12x 10G BASE-T oraz 12x1000/10GBASE-X SFP+ port |  | |
| **Rodzaj urządzenia** | przełącznik warstwy L3 |  | |
| **Przepustowość przełączania** | Min. 480 Gbit/s |  | |
| **Przepustowość** | Min. 350 Mpps |  | |
| **Pamięć RAM** | Min. 1 GB |  | |
| **Pamięć flash** | Min. 256 MB |  | |
| **MAC addresses** | 16 000 |  | |
| **Inne** | obsługa ssl/ssh; pełny dupleks, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).  Możliwość łączenia w stos za pomocą interfejsów 10Gb/s. |  | |
| **Akcesoria** | Zamawiający wymaga dostarczenia wraz z przełącznikiem:  12 x Transceiver SFP+ 10GBASE-LR 10km |  | |
| **Gwarancja** | Min. 36 miesięcy |  | |

1. **Przełącznik** **zarządzający – Producent ……………… / model ………………..**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRZEŁĄCZNIK ZARZĄDZAJĄCY** | | **Ilość** | **1 sztuka** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| **Obudowa** | Umożliwiająca montaż w szafie rack 19” |  | |
| **Liczba gniazd** | 24 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne |  | |
| **Rodzaj urządzenia** | przełącznik warstwy L3 |  | |
| **Przepustowość przełączania** | Min. 128 Gbit/s |  | |
| **Przepustowość** | Min. 95,2 Mpps |  | |
| **Pamięć RAM** | Min. 1 GB |  | |
| **Pamięć flash** | Min. 256 MB |  | |
| **MAC addresses** | 16 000 |  | |
| **Inne** | obsługa ssl/ssh; pełny dupleks, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).  Możliwość instalacji drugiego modularnego zasilacza. |  | |
| **Akcesoria** | Zamawiający wymaga dostarczenia wraz z przełącznikiem:  2x Transceiver SFP+ 10GBASE-LR 10km |  | |
| **Gwarancja** | Min. 36 miesięcy |  | |

1. **Przełącznik dostępowy – Producent …………………. / model ……………………**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRZEŁĄCZNIK DOSTĘPOWY** | | **Ilość** | **10 sztuk** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| **Obudowa** | Umożliwiająca montaż w szafie rack 19” |  | |
| **Liczba gniazd** | 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne |  | |
| **Rodzaj urządzenia** | przełącznik warstwy L3 |  | |
| **Przepustowość przełączania** | Min. 176 Gbit/s |  | |
| **Przepustowość** | Min. 130 Mpps |  | |
| **Pamięć RAM** | Min. 1 GB |  | |
| **Pamięć flash** | Min. 256 MB |  | |
| **MAC addresses** | 16 000 |  | |
| **Inne** | obsługa ssl/ssh; pełny dupleks, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).  Możliwość instalacji drugiego modularnego zasilacza. |  | |
| **Akcesoria** | Zamawiający wymaga dostarczenia wraz z przełącznikiem:  2x Transceiver SFP+ 10GBASE-LR 10km |  | |
| **Gwarancja** | Min. 36 miesięcy |  | |

1. **Kontroler WIFI - Producent …………………. / model ……………………**

|  |  |  |  |
| --- | --- | --- | --- |
| **KONTROLER WiFi** | | **Ilość** | **1 sztuka** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry** | |
| **Obudowa** | Umożliwiająca montaż w szafie rack 19”. |  | |
| **Liczba gniazd** | * 4 x RJ45 Gigabit oraz RS232 * Minimum 2 porty USB |  | |
| **Pozostałe** | * Kontroler powinien mieć możliwość obsługi do 30 punktów dostępowych, * Kontroler powinien mieć możliwość rozbudowy obsługi do 50 punktów dostępowych, * Kontroler powinien mieć możliwość zabezpieczenia przed awarią za pomocą redundantnego kontrolera. Klaster stworzony z dwóch kontrolerów powinien być realizowany za pomocą protokołu VRRP, * Kontroler sieci bezprzewodowej powinien mieć możliwość zarządzania punktami dostępowymi obsługującymi 802.11 A/B/G/N/AC, * Rozwiązanie powinno mieć możliwość skalowania poprzez stos do 150 punktów dostępowych, * Kontroler powinien umożliwić obsługę minimum 128 profili bezpieczeństwa SSID, * Maksymalna ilość obsługiwanych użytkowników na kontroler powinna wynieść minimum 2000, na klaster 6000, * Kontrola przepustowości na SSID oraz klienta, * Kontroler powinien być wyposażony w aplikację umożliwiającą zaplanowanie ilości oraz rozmieszczenia punktów dostępowych na mapie dostarczonej przez zamawiającego. Aplikacja powinna być częścią składową wewnętrznego oprogramowania, * Kontroler powinien obsługiwać Captive portal, * Urządzenie powinno obsłużyć minimum 64 VLAN oraz jeden VLAN administracyjny, * Możliwość automatycznego planowania częstotliwości oraz ilości AP  w celu objęcia zasięgiem danego obszaru, * Powiadamianie o niepokrytych sygnałem radiowym obszarach oraz możliwość wypełnienia tych obszarów sąsiednimi punktami dostępowymi * Automatyczna konfiguracja kanałów radiowych w punkcje dostępowym w celu redukcji interferencji, * Automatyczne zarządzanie siłą sygnału w zależności od obszaru jaki dany punkt dostępowy ma pokryć, * Możliwość "przeniesienia" użytkownika pomiędzy punktami dostępowymi w przypadku zbyt dużego obciążenia punktu dostępowego. |  | |
| **Gwarancja** | Wymaga się, aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta.  Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii  z wysyłką w następnym dniu roboczym po stwierdzeniu awarii. |  | |

1. **Punkt dostępowy - Producent …………………. / model ……………………**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PUNKT DOSTĘPOWY** | | **Ilość** | | **25 sztuk** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | | **Oferowane parametry** | |
| **Ogólne** | Urządzenie typu access-point przeznaczone do montażu wewnątrz budynku musi być zgodne ze standardam IEEE 802.11ac min. 2.4GHz (300Mbps) oraz 5GHz (867Mbps).  Zarządzanie access-pointem musi odbywać się za pomocą dedykowanego kontrolera sprzętowego dostarczonego przez producenta access-pointa Wyposażony w co najmniej wewnętrzne anteny 5/6dBi (2.4/5GHz). | |  | |
| **Wymagania** | * WMM Wireless Multimedia Prioritization, * WDS Wireless Distribution System, * Pobór mocy max 11W, * Power over Ethernet (PoE) IEEE 802.3af/802.3at, * Z uwagi na miejsce montażu waga punktu dostępowego nie może przekraczać 800g, * Min. jeden port 10/100/1000BASE-T, * Port konsoli ze złączem RJ45, * Dwa gniazda SMA z odwróconą polaryzacją na dwupasmowe (2,4 i 5 GHz) anteny zewnętrzne, * WiFi Protected Access (WPA, WPA2), * 64/128/152-bitowe szyfrowanie Wired Equivalent Privacy (WEP), * IEEE 802.1x RADIUS, protokoły uwierzytelniania EAP TLS, TTLS, PEAP, * Kontrola dostępu bezprzewodowego poprzez identyfikację autoryzowanych urządzeń sieci bezprzewodowej, * Uwierzytelnianie sprzętowym adresem MAC, * Obsługa funkcji VPN pass-through, * Zdalne zarządzanie zabezpieczone protokołem Security Sockets Layer (SSL), * Zarządzanie w pozwalające obsługiwać nawet 10 punktów dostępowych  w ramach jednej grupy, * Zarządzanie przez SNMP obsługuje SNMP MIB II, 802.11 MIB  i opatentowaną konfigurację MIB. | |  | |
| **Instalacja** | Wykonawca uzgodni z Zamawiającym miejsce instalacji punktów dostępowych zgodnie z wytycznymi opisanymi w dokumencie.  Wraz z punktami dostępowymi należy dostarczyć wszystkie niezbędne akcesoria wymagane do poprawnej pracy urządzenia w tym, dedykowany zasilacz, zestaw do montażu na ścianie lub suficie. | |  | |
| **Gwarancja** | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta.  Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii  z wysyłką w następnym dniu roboczym po stwierdzeniu awarii. | |  | |

……………………….., dn. ……………….

.............................................

podpis i pieczątka imienna osoby

upoważnionej do reprezentowania Wykonawcy