Załącznik nr 6 do SWZ – Szczegółowy opis przedmiotu zamówienia

Szczegółowy Opis Przedmiotu Zamówienia

Dostawa sprzętu komputerowego: serwera AD, plików i maszyn wirtualnych, serwera backupowego NAS, urządzenia UTM i zasilacza UPS dla Urzędu Miejskiego w Cieszynie.

Przedmiotem zamówienia jest dostawa sprzętu komputerowego: serwera AD, plików i maszyn wirtualnych, serwera backupowego NAS, urządzenia UTM i zasilacza UPS o parametrach podanych w wymaganiach techniczno-funkcjonalnych i zabezpieczeń.

1. **Wymagane parametry techniczne proponowanych rozwiązań:**
   1. **Serwer — domena AD, serwer plików i maszyn wirtualnych**

      Serwer nowy, nie powystawowy, nie odnowiony, wolny od obciążeń prawami osób trzecich, w obudowie typu RACK nie większej niż 2U do szafy 19” (pełny osprzęt umożliwiający montaż), który będzie wykorzystywany do utworzenia domeny AD Windows Server 2022 Standard i serwera plików dla jej klientów (minimum 30 użytkowników) z możliwością postawienia 2 maszyn wirtualnych Windows Server 2022 Standard (z licencjami dostępowymi dla klientów domeny) z usługami np. IIS, darmową wersją MS SQL, oprogramowaniem/usługami firm trzecich, oraz 2 maszyn wirtualnych Linux z serwerami baz danych Firebird, PostgreSQL.

      Wymagane parametry techniczne:

      możliwość montażu w szafie RACK 19” 1-2U

      procesor: 1-2 procesory 64-bit minimum 16 rdzeni łącznie, zaprojektowany do pracy w serwerach, o wydajności co najmniej 35000 punktów każdy na podstawie PassMark Performance Test w teście PassMark – CPU Mark według wyników opublikowanych na stronie (dnia 02.07.2024 r.): http://www.cpubenchmark.net/cpu_list.php

      pamięć operacyjna RAM: minimum 128GB

      pamięć masowa:

      minimum 800GB SSD SAS dostępne w RAID 1 na system operacyjny, hot plug

      minimum 8TB SSD SATA dostępne w RAID 6 przestrzeni dyskowej na dane, hot plug

      karta graficzna: zintegrowana lub dedykowana

      moduł TPM 2.0

      karty sieciowe:

      minimum 4x1Gb RJ45

      minimum 2x10Gb RJ45

      zarządzanie:

      Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden dedykowany port 100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł musi umożliwiać monitorowanie podzespołów serwera oraz posiadać wbudowane narzędzia diagnostyczne. Całe rozwiązanie z oprogramowaniem do zdalnego

zarządzania serwerem musi być produktem pochodzącym od producenta serwera oraz musi być objęte wsparciem producenta serwera.

sprzętowe wspomaganie wirtualizacji

zasilanie: dwa redundantne zasilacze o odpowiedniej mocy dla zaproponowanego serwera

oprogramowanie: Windows Server 2022 Standard PL 64bit, z licencją na zaproponowaną liczbę rdzeni, lub równoważny serwerowy system operacyjny

30 sztuk licencji dostępowych dedykowanych do systemu operacyjnego serwera

gwarancja: NBD 36 miesięcy, zachowanie dysków twardych przy awarii

certyfikaty: CE (Conformité Européenne), ISO-9001:2015

zapasowe dyski: 1x SAS, 2x SATA (jako rezerwowe dla zastosowanych w proponowanym serwerze)

2. **Serwer backupowy NAS**

Serwer NAS nowy, nie powystawowy, nie odnowiony, wolny od obciążeń prawami osób trzecich, w obudowie typu RACK nie większej niż 2U (pełny osprzęt umożliwiający montaż), który będzie wykorzystywany do tworzenia kopii danych z serwerów domenowych Windows 2022, bazodanowych oraz kopii maszyn wirtualnych Hyper-V.

Wymagane parametry techniczne:

możliwość montażu w szafie RACK 19” 1-2U

pamięć systemowa: minimum 16GB RAM

procesor: minimum 4-rdzeniowy, 64-bitowy procesor

zasilanie: dwa redundantne zasilacze o odpowiedniej mocy dla proponowanego rozwiązania

karty sieciowe: minimum 2 porty 1GB

obsługa RAID: 0, 1, 5, 6, 10

powierzchnia dyskowa: minimum 10TB dostępnej powierzchni dyskowej dysków połączonych w RAID 6

oprogramowanie: oprogramowanie do robienia kopii zapasowych plików użytkowników domeny (kopia przyrostowa i lustrzana), udostępnianych udziałów sieciowych, maszyn wirtualnych Hyper-V Windows 2022

gwarancja: minimum 36 miesięcy, zachowanie dysków twardych przy awarii

certyfikaty: CE (Conformité Européenne), ISO-9001:2015

zapasowe dyski: dwa zapasowe dyski dla zastosowanych w proponowanym serwerze NAS

3. **Urządzenie UTM**

Urządzenie klasy UTM nowe, nie powystawowe, nie odnowione, wolne od obciążeń prawami osób trzecich, w obudowie typu RACK do szafy 19” (pełny osprzęt umożliwiający montaż).

Urządzenie ma zabezpieczać połączenie z internetem, umożliwiać filtrowanie ruchu wychodzącego i przychodzącego, monitorować i blokować dostęp do stron i usług internetowych na podstawie udostępnianych przez producenta i własnych filtrów, zapobiegać atakom internetowym, blokować zagrożenia związane z korzystaniem z maili i wirusami komputerowymi, blokować niechciane aplikacje, umożliwiać połączenia VPN z pełną autoryzacją i logowaniem działań użytkowników.

Wymagane parametry techniczne:

Interfejsy:

1. Urządzenie musi posiadać co najmniej poniższą liczbę i rodzaj interfejsów:
   minimum 10 portów Gigabit Ethernet RJ-45.
   minimum 8 gniazd SFP 1 Gbps.
   minimum 4 gniazd SFP+ 10 Gbps.
2. Musi pozwalać skonfigurować co najmniej 200 interfejsów VLAN w oparciu o standard 802.1Q.

Wydajność:

1. Firewall musi obsługiwać nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side, jak i server side w ramach modułu IPS) - minimum 5 Gbps.
6. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, kontrola aplikacji, antywirus — minimum 2.5 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje bezpieczeństwa:

System musi realizować wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu — zapora ogniowa klasy Stateful Inspection
2. Kontrola aplikacji
3. Poufność transmisji danych — połączenia szyfrowane IPSec VPN oraz SSL VPN
4. Ochrona przed malware
5. Ochrona przed atakami — Intrusion Prevention System
6. Kontrola stron WWW
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS, jak i w ruchu przechodzącym przez system.
13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (np. wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki Firewall:

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   1. Translację jeden do jeden oraz jeden do wielu.
   2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

Połączenia VPN:

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
    1. Wsparcie dla IKE v1 oraz v2.
    2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode (GCM).
    3. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    4. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    5. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    6. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
    7. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
    8. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
    9. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    10. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
    1. Pracę w trybie Portal — gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
    2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
    3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN:

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN:

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne, jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem:

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware:

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
6. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
7. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami:

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DdoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injection, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji:

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW:

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji:

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
    1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie:

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora, w CLI lub GUI, które nie zostaną zaimplementowane, zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie:

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne:

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje:

Jeśli wymagane są licencje do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów ich koszt musi być objęty ofertą na okres minimum 36 miesięcy (np. kontrola aplikacji, IPS, antywirus, filtrowanie ruchu sieciowego na podstawie baz danych adresów sieciowych IP, FQDN)

Gwarancja oraz wsparcie:

System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Szkolenie z konfiguracji UTM:

1. Wykonawca (trener) musi posiadać certyfikat producenta oferowanego sprzętu,
2. Wykonawca przeprowadzi szkolenie łącznie minimum 12 godzin (szkolenie w formie zdalnej).
3. Po zakończeniu szkolenia zostaną wystawione dla przeszkolonych pracowników certyfikaty potwierdzające odbycie szkolenia.
4. Wykonawca oprze szkolenie na minimum następującej agendzie:
    - Konfiguracja trybów pracy urządzenia (transparentny/sniffer lub router/NAT)
    - Zarządzanie aktualizacjami oraz backup.
    - Budowa i optymalizacja reguł zapory sieciowej.
    - Konfiguracja systemu wykrywania włamań (IDS/IPS).
    - Monitorowanie wykorzystania aplikacji i blokowanie malware/ransomware.
    - Konfiguracja modułu filtrowania stron www.
    - Konfiguracja profili antyspam.

- Zarządzanie wyciekiem danych DLP.
- Konfiguracja wielu łączy internetowych WAN.
- Raportowanie i analiza zdarzeń.
- Zaawansowana konfiguracja wielu łącz internetowych – SD WAN.
- Konfiguracja połączeń tunelowych Site-to-Site IPsec VPN.
- Zarządzanie dostępem zdalnym SSL- VPN w oparciu o dwu stopniowe metody uwierzytelniania.
- Zarządzanie mechanizmami routingu.
- Konfiguracja systemów ochrony przed atakami DDoS.
- Zaawansowana analiza logów i zdarzeń.
- Diagnostyka i rozwiązywanie problemów.

Opisy do wymagań ogólnych:

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument — oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

4. UPS

Zasilacz UPS nowy, nie powystawowy, nie odnowiony, wolny od obciążeń prawami osób trzecich, w obudowie typu RACK do szafy 19” (pełny osprzęt umożliwiający montaż), wymagana minimalna moc zasilacza UPS 4kW, wraz z akumulatorami, zapewniającego podtrzymanie zasilania minimum 60 minut dla obciążenia mocą 80% mocy zasilacza.

Wymagane parametry techniczne:

możliwość montażu w szafie RACK 19”

moc rzeczywista: minimum 4kW

port komunikacyjny USB lub LAN do obsługi i zarządzania UPS-em

oprogramowanie do zarządzania UPS kompatybilne z systemem operacyjnym Windows

minimum 4 gniazd wyjściowych

czas podtrzymania: przy 80% obciążenia – minimum 60 minut

system automatycznej regulacji napięcia AVR

styk EPO (wyłączenie awaryjne)

baterie w komplecie – UPS gotowy do pracy/rozruchu

gwarancja: minimum 36 miesięcy

2. **Gwarancja:**

Gwarancja na wszystkie składniki zamówienia minimum 3 lata (36 miesięcy).