

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. Ogólna charakterystyka i warunki realizacji zamówienia:

1. Dostawa fabrycznie nowego sprzętu komputerowego wchodzącego w skład Urządzeń sieciowych na potrzeby RCIM
2. **Zamawiający nie dopuszcza składanie ofert częściowych, gdzie część (zadanie) stanowi:**
 - a. **Zadanie częściowe nr 1** – dostawa fabrycznie nowego sprzętu komputerowego-Urządzenie sieciowe typu UTM.
 - b. **Zadanie częściowe nr 2** – dostawa fabrycznie nowego sprzętu komputerowego-Urządzenie sieciowe typu Router.
3. Przedmiotem zamówienia jest:
 - a) dostarczenie do siedziby Zamawiającego przedmiotu zamówienia zgodnego z OPZ,
 - b) udzielenie niezbędnych licencji na oprogramowanie,
 - c) dostarczone Urządzenia sieciowe będą posiadały najnowsze stabilne na dzień dostawy Oprogramowanie układowe udostępniany przez producenta urządzenia,
 - d) dostarczenie instrukcji obsługi przedmiotu zamówienia, w języku polskim lub angielskim,
 - e) udzielenie gwarancji na dostarczony przedmiot zamówienia
 - f) wykonanie czynności umożliwiających uruchomienie wsparcia gwarancyjnego dla Urządzeń sieciowych, łącznie z potwierdzoną rejestracją, mającą status aktywny na stronach www producentów tych Urządzeń sieciowych. Wsparcie o którym mowa ma mieć status aktywny na stronie www producenta, nie później niż od dnia podpisania protokołu odbioru Urządzeń sieciowych.
 - g) zapewnienie uaktualnień Oprogramowania układowego oraz uaktualnień Licencji i subskrypcji UTM, producenta danego Urządzenia sieciowego, zgodnie ze złożoną ofertą.
 - h) w ramach gwarancji, wykonawca zobowiązany jest wykonać aktualizację Oprogramowania układowego Urządzeń sieciowych, nie rzadziej niż raz w danym roku kalendarzowym, w terminie uzgodnionym z Zamawiającym lub Administratorem RCIM. Zakłada się, że pierwszym rokiem w którym nastąpi instalacja Oprogramowania układowego jest rok 2020.
4. Oferowany sprzęt i oprogramowanie musi być objęte gwarancją producenta przez okres zgodny ze złożoną ofertą, jednak nie krótszy niż zawarty w opisie wymagań minimalnych. Okres gwarancji będzie liczony od daty podpisania protokołu odbioru.
5. Naprawy będą dokonywane w miejscu eksploatacji Urządzeń sieciowych,
6. Wszelkie koszty usunięcia Awarii (usług, części, sprzętu zastępczego i transportu) ponosi Wykonawca,
7. Producent oferowanego sprzętu musi zapewnić wysoki poziom wsparcia technicznego, co zostanie potwierdzone przez:
 - a) Oferowane produkty muszą spełniać wszystkie parametry określone w niniejszym załączniku oraz być fabrycznie nowe, oznakowane symbolem CE, pochodzić z legalnego źródła, muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych

zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski. Wraz z dostawą należy załączyć informację od producenta potwierdzającą, że dostarczane urządzenie o numerach seryjnych pochodzą z autoryzowanego kanału sprzedaży producenta i zostały wyprodukowane nie dawniej niż 3 miesiące przed ich dostarczeniem. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia urządzenia w postaci oświadczenia producenta. Pochodził z bieżącej oferty producenta przeznaczonej na rynek Unii Europejskiej. Był fabrycznie nowy, tj. fabrycznie zapakowany, nieużywany w innych projektach, ani testach. Nie dopuszcza się produktów prefabrykowanych i odnawianych.

- 8. Wymaga się, aby funkcjonalności zdefiniowane w opisie minimalnych wymagań dla danego Urządzenia sieciowego, były zrealizowane w postaci jednolitej zamkniętej platformy sprzętowej wchodzącej w skład danego Urządzenia sieciowego wykonanego przed producenta tego Urządzania sieciowego.**
9. Wykonawca winien przedstawić nazwę, producenta i model oferowanego sprzętu i oprogramowania w poszczególnych jego rodzajach.
10. W stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), po podpisaniu umowy Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, że 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 p. 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.
11. Sprzęt i jego komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
12. Do każdego Urządzenia sieciowego musi być dostarczony komplet nośników umożliwiających odtworzenie Oprogramowania układowego zainstalowanego w Urządzeniu sieciowym.
13. Przedmiot zamówienia musi pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
14. Przed dostawą Urządzeń sieciowych, muszą być one zarejestrowane przez producenta, bezpośrednio na Zamawiającego, jako jedyne go użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji produkowanego sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.
15. Zamawiający może zażądać od Wykonawcy, przed dostawą przedmiotu zamówienia, dokumentu zawierającego listę numerów seryjnych dostarczanych Urządzeń sieciowych, w celu weryfikacji spełnienia warunków licencyjnych oraz gwarancyjnych.
16. Zamawiający zastrzega sobie prawo do sprawdzenia spełnienia zakresu uprawnień licencyjnych oraz gwarancyjnych, w polskim biurze producenta na podstawie numeru

seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.

III Opis minimalnych wymagań

1. Urządzenie sieciowe typu UTM – szt. 1

- a. Urządzenie typu Rack 19”
- b. Urządzenie powinno dysponować portami minimum 16 x GE RJ45 (16 x LAN, 2 x GE SFP).
- c. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC lub MIPS.
- d. Urządzenie musi być dostarczone z licencją producenta „na urządzenie” - bez limitu chronionych użytkowników i urządzeń w sieci wewnętrznej.
- e. Wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny mają pochodzić od jednego producenta.
- f. Połączenie dwóch identycznych urządzeń w klaster typu Active-Passive.
- g. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
- h. System ochrony musi obsługiwać w ramach jednego urządzenia minimum następujące funkcjonalności podstawowe:
 - kontrolę dostępu - zaporę ogniową klasy Stateful Inspection,
 - ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, HTTPS, FTP, IM),
 - poufność danych - IPSec VPN oraz SSL VPN,
 - ochronę przed atakami - Intrusion Prevention System [IPS/IDS], oraz funkcjonalności uzupełniających:
 - kontrolę treści – Web Filter [WF],
 - kontrolę pasma oraz ruchu [QoS i Traffic shaping],
 - kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P),
 - zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Prevention).
 - monitoring, wykrywanie i alarmowanie o uszkodzeniu elementów sprzętowych i programowych systemu zabezpieczeń oraz łącz sieciowych.
- i. Urządzenie ma dawać możliwość ustawienia jednego z dwóch trybów pracy:

- jako router/NAT (3 warstwa ISO-OSI),
- jako most/transparent bridge - tryb przezroczysty umożliwiający wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.

j. Polityka bezpieczeństwa systemu zabezpieczeń (firewall) musi uwzględniać minimum:

- adresy IP,
- interfejsy,
- protokoły i usługi sieciowe,
- użytkowników sieci,
- reakcje zabezpieczeń,
- rejestrowanie zdarzeń i alarmowanie o nich,
- zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ),
- urządzenia muszą obsługiwać nie mniej niż 10 000 polityk firewall,
- urządzenia muszą wykrywać i blokować ataki/techniki ataków stosowanych przez hakerów/krakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan, DDoS) i niebezpiecznych komponentów (m.in. Java/ActiveX),
- urządzenia muszą zapewnić ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP,
- aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie,
- ma być zapewniona możliwość wykrywania anomalii protokołów i ruchu,
- system zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą co najmniej następujących parametrów:
- haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia,
- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
- haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych.

k. Rozwiązanie ma umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.

l. Wydajność:

- zapewnienie możliwości obsługi min. 2 000 000 jednoczesnych połączeń i min. 14 000 nowych połączeń na sekundę,

- przepływność nie mniejsza niż 3,75 Gbps (dla pakietów o wielkości 1518) dla ruchu nieszyfrowanego,
- wydajność ruchu dla IPS nie mniejsza niż 1,8 Gbps
- umożliwienie obsługi min. 1000 jednoczesnych tuneli VPN IPSec w trybie Client to Gateway oraz min. 500 w trybie SSL VPN.

m. Konfiguracja i zarządzanie:

- ma być umożliwiona konfiguracja systemu poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI),
- dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji,
- musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach.
- Administratorzy muszą być uwierzytelniani za pomocą: haseł statycznych, haseł dynamicznych (RA, RADIUS, RSA SecureID),
- system ma umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji
- dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta,
- system/urządzenia powinny mieć możliwość współpracy z zewnętrznym kompatybilnym modulem centralnego zarządzania umożliwiającym co najmniej: przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej, zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia, monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM), zapis i zdalne wykonywanie skryptów na urządzeniach.

n. Możliwość rozbudowy:

- system powinien mieć możliwość współpracy z zewnętrznym modulem raportowania i korelacji logów umożliwiającym: zbieranie logów z urządzeń bezpieczeństwa, generowanie raportów
- w/w funkcjonalności powinny być zarządzane poprzez jedną wspólną konsolę do kontroli obu podsystemów.

o. Urządzenie musi umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

p. W ramach funkcji IPSec VPN, SSL VPN – producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.

r. Urządzenie jest nielimitowane na użytkowników.

s. Urządzenie ma używać pamięci FLASH o pojemności nie mniejszej niż 32 GB.

t. Urządzenie musi zawierać osprzęt niezbędny do prawidłowej instalacji w szafie typu Rack 19”.

2. Urządzenie sieciowe typu Router – szt. 1

- a. Urządzenie typu rack 19” o architekturze modularnej, wyposażone w 6 portów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP lub równoważnych, a także w 2 porty 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+.
- b. Urządzenie musi posiadać 8 portów 1 Gigabit Ethernet. Wszystkie porty muszą być wyposażone we wkładki typu SFP-GE-T 1000BASE-T SFP lub równoważne.
- c. Urządzenie umożliwia rozszerzenie m.in. o następujące porty:
- d. Urządzenie posiada zasoby sprzętowe pozwalające przełączać 19 Mpps oraz 20 Gbps ruchu.
- e. Urządzenie domyślnie pozwala na przełączanie z prędkością 2,5 Gbps i umożliwia licencyjne odblokowanie wydajności do wartości 20 Gbps.
- f. Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność 5 Gbps dla ruchu IMIX.
- g. Urządzenie posiada 8 GB pamięci RAM.
- h. Urządzenie obsługuje 1 000 000 prefiksów w tablicach ruting IPv4.
- i. Urządzenie obsługuje 1 000 000 prefiksów w tablicach ruting IPv6.
- j. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.
- k. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.
- l. Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.
- m. Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routing Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.
- n. Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.
- o. Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.
- p. Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN.
- q. Urządzenie obsługuje protokół NHRP (ang. Next Hop Resolution Protocol).
- r. Urządzenie obsługuje protokół GDOI (RFC 3547).
- s. Funkcjonalności związane z niezawodnością pracy:
- a) system modułowy umożliwiający aktualizację poszczególnych modułów programowych niezależnie od siebie

- b) redundancja procesów routingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego
- c) BFD dla OSPF, BGP, ISIS
- d) IP FRR
- e) BGP Prefix-Independent Convergence (PIC)
- f) Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP
- g) funkcjonalność VRRP
- h) redundantne zasilacze 220V
- i) możliwość wymiany modułów w trakcie pracy (ang. hot swap)
- t. Urządzenie obsługuje MPLS, w szczególności:
 - a) a LDP
 - b) b. EoMPLS, VPLS
 - c) 6. MPLS L3 VPN
 - d) d. MPLS TE
 - e) e. MPLS FRR w trybach protekcji łącza oraz węzła
- u. Urządzenie obsługuje następujące mechanizmy jakości usług (QoS):
 - a) klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per por VLAN zarówno dla IPv4 jak i IPv6
 - b) hierarchiczny QoS (H-QoS) 3 poziomy
 - c) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP
 - d) dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek
 - e) algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek
 - f) możliwość obsługi jednej kolejki z priorytetem w stosunku do innych
 - g) mechanizm ograniczania ilości ruchu w kolejce priorytetowej
 - h) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP — poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
 - i) możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting)
 - j) mechanizm WRED
 - k) możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS
- v. Urządzenie obsługuje następujące funkcje i elementy bezpieczeństwa:
 - a) sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu
 - b) Unicast RPF (Reverse Path Forwarding)
 - c) listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
 - d) 30 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), a także 4.000 list kontroli dostępu (ACL)
 - e) dostęp administracyjny oparty o role z przypisanymi uprawnieniami
 - f) zasoby sprzętowe umożliwiające uruchomienie funkcjonalności zapory ogniowej typu stateful (ang. stateful firewall), przy czym zaporą ogniową:

- umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji)
- obsługuje ruch IPv4 oraz IPv6
- umożliwia konfigurację polityk per wirtualna tablica routingu (VRF)
- umożliwia obsługę 2 000 000 równoczesnych sesji
- umożliwia zestawianie 200 000 nowych połączeń HTTP na sekundę
- g) zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością 5 Gbps (AES256) z obsługą 8 000 tuneli IPSec
- h) sieci VPN typu site-2-site oparte o IPSec
- i) dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmisji danych pomiędzy oddziałami
- j) bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast
- k) algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:
 - Elliptic Curve Diffie-Hellman (ECDH)
 - Galois Counter Mode Advanced Encryption Standard (GCM-AES) 128/256 bitów
 - Galois Message Authentication Code (GMAC-AES) 128/256 bitów
 - Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2
- l) konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2
 - IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych
 - IKEv2 zarówno dla ruchu IPv4 jak i IPv6
- m) funkcjonalność VPN per VRF
- n) ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU
- o) logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU
- p) możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków
- w. Urządzenie musi być dostarczone wraz z odpowiednimi licencjami bezpieczeństwa zapewniając obsługę funkcjonalności szyfrowania IPSec oraz funkcjonalności zapory ogniowej typu stateful (ang. stateful firewall) opisanych powyżej
- x. Urządzenie umożliwia uruchomienie usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, przy czym klasyfikacja ta:
 - a) opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji/protokołów
 - b) udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurację QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji).
 - c) nie wymaga rozbudowy sprzętowej urządzenia, jedynie zakup licencji
- y. Urządzenie obsługuje 4000 tuneli GRE.

- z. Urządzenie posiada możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.
- aa. Urządzenie umożliwia ochronę kryptograficzną tuneli GRE.
- bb. W ramach funkcjonalności zarządzania, urządzenie:
 - a) umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
 - b) obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802. lag. ITU-T Y.1731)
 - c) obsługuje MPLS OAM
 - d) umożliwia pisanie skryptów konfiguracyjnych
 - e) obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6
 - f) posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP
 - g) posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
 - h) posiada dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX
 - i) posiada port USB
 - j) posiada możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej
- konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona
- k) urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów
- cc. Urządzenie posiada redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia.
- dd. Urządzenie umożliwia montaż w szafie 19". Dostarczany sprzęt musi być objęty min. 12-miesięcznym (1 rok) serwisem opartym na serwisie producenta urządzenia świadczonym w reżimie 24x7x4.
- ee. Urządzenie musi zawierać osprzęt niezbędny do prawidłowej instalacji w szafie typu Rack 19".

IV Charakterystyka dostaw:

1. Dostawa sprzętu i oprogramowania nastąpi zgodnie ze specyfikacją i na warunkach określonych poniżej:

- a) Dostawa zostanie zrealizowana przez wykonawcę w terminie nie dłuższym niż 30 dni, liczonych od dnia podpisania Umowy. Dostarczony sprzęt będzie fabrycznie nowy, kompletny, nie używany w innych projektach oraz zapakowany przez producenta, w szczególności nie dopuszcza się produktów „odnawianych” (ang. Refurbished).
- b) Dostawy przedmiotu zamówienia, będą się odbywać w Dni robocze w godzinach od 8.00 do 14.00.
- c) W przypadku stwierdzenia przez uprawnionego pracownika Zamawiającego wad, Zamawiający nie dokona odbioru całości dostawy. Wykonawca będzie wówczas zobowiązany do dostarczenia na własny koszt całości dostawy, wolnej od wad.

- d) Dostawę uważa się za zakończoną co do całości lub części dostawy po podpisaniu dokumentu potwierdzającego ten fakt protokołem odbioru, niezawierającego żadnych zastrzeżeń co do uszkodzeń lub braków ilościowych dostawy przedmiotu umowy.