Załącznik nr 1.1 do SIWZ

Szczegółowy opis przedmiotu zamówienia na dostawę sprzętu teleinformatycznego na potrzeby modernizacji systemu ASG-EUPOS

Część 1 zamówienia – dostawa sprzętu sieciowego na potrzeby centrum zarządzającego ASG-EUPOS

I Informacje ogólne

1. Zamówienie obejmuje dostawę wraz z instalacją sprzętu sieciowego na potrzeby rozbudowy i utrzymania systemu ASG-EUPOS.
2. Wykonawca zobowiązany jest dostarczyć do wskazanych lokalizacji Zamawiającego i zainstalować niżej wymieniony sprzęt i oprogramowanie zgodne ze specyfikacją opisaną poniżej.
   1) Urządzenie UTM (unified threat management) – 1 szt.
   2) Router – 1 szt.
   3) Przełącznik – 2 szt.
3. Dostarczony przez Wykonawcę sprzęt musi być fabrycznie nowy i oryginalnie zapakowany.

II Specyfikacja techniczna sprzętu i oprogramowania

1. Urządzenie UTM– 1 szt.

Tabela 1 Minimalne, wymagane parametry techniczne urządzenia UTM

Lp	Nazwa	Parametry minimalne
1	Architektura	Dostarczony system bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje bezpieczeństwa. Urządzenie w obudowie umożliwiającej montaż w szafie RACK. Wraz z urządzeniem Wykonawca dostarczy elementy potrzebne do montażu urządzenia w szafie RACK. Możliwość łączenia urządzeń w klaster typu Active-Active lub Active-Passive
2	Funkcjonalności	1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 2. Monitoring stanu realizowanych połączeń VPN. 3. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. 4. System realizujący funkcję Firewall powinien dysponować minimum 8 portami Ethernet 10/100/1000 Base-TX , 8 gniazdami SFP 1Gbps. 5. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 6. W zakresie Firewall'a obsługa nie mniej niż 6 milionów jednoczesnych połączeń oraz 210 tys. nowych połączeń na sekundę 7. Przepustowość Firewall'a: nie mniej niż 16 Gbps 8. Wydajność szyfrowania VPN IPSec: nie mniej niż 14 Gbps 9. System powinien być wyposażony w lokalny dysk o pojemności minimum 120 GB, który może być wykorzystany do celów logowania i raportowania. W przypadku braku lokalnego dysku, system powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy

		sprzętowej lub programowej. 10. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. 11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji: a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection b. Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN d. Ochrona przed atakami - Intrusion Prevention System e. Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. f. Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP g. Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma h. Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C) i. Możliwość analizy ruchu szyfrowanego protokołem SSL j. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) k. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. 12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 4,5 Gbps 13. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, AC, AV - minimum 2 Gbps 14. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: a. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site b. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności c. Praca w topologii Hub and Spoke oraz Mesh d. Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF e. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth 15. W ramach funkcji IPSec VPN, SSL VPN – producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 16. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 17. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a (w przypadku zakupu minimum dwóch urządzeń). 18. Translacja adresów NAT adresu źródłowego i docelowego. 19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci. 20. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ

		21. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. 22. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. 23. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP 24. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW. 25. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. 26. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu b. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP c. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory 27. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: a. ICSA lub EAL4 dla funkcji Firewall b. ICSA lub NSS Labs dla funkcji IPS c. ICSA dla funkcji: SSL VPN, IPSec VPN 28. Systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3	Serwisy i licencje	W ramach zamówienia Wykonawca dostarczy licencje aktywacyjne dla wszystkich wymienionych funkcjonalności, uprawniające do używania ww. funkcji oraz pobierania aktualizacji baz zabezpieczeń minimum w okresie gwarancji.
4	Wyposażenie	Razem z urządzeniem Wykonawca dostarczy: - wkładki do portów SFP do połączeń światłowodowych typu 1GE SX – 8 szt. - wkładki do portów SFP do połączeń miedzianych typu 1GE Copper Transceiver – 8 szt. - 8 szt. patchcordów światłowodowych o długości od 2 do 3 m typu LC-LC, kompatybilnych z dostarczonymi wkładkami światłowodowymi

		- 8 szt. patchcordów miedzianych RJ45, CAT 6 o długości 3 m. - komplet przewodów zasilających, z zakończeniem typu DIN49441.
4	Kompatybilność	1. Urządzenie UTM zapewni bezproblemową współpracę z urządzeniami typu UTM / FireWall posiadanymi przez Zamawiającego (FortiNet FortiGate800A, Juniper Netscreen 5GT ADSL, Juniper SSG5, Juniper SSG20, Juniper SRX110) w zakresie zestawiania i utrzymywania połączeń VPN IPSec.
5	Gwarancja	1. Gwarancja na bazie świadczenia gwarancyjnego producenta sprzętu przez okres minimum 36 miesięcy. Wykonawca zapewnia, że dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji producenta sprzętu. Z dostawą sprzętu Wykonawca zobowiązuje się dostarczyć dokument wydany przez producenta lub jego polskiego przedstawiciela, potwierdzający że sprzęt jest nowy (potwierdzająca data produkcji), pochodzi z oficjalnego kanału dystrybucji, pochodzi z bieżącej produkcji i objęty jest wsparciem serwisowym producenta przez okres wymagany w SIWZ. 2. Okres gwarancji rozpoczyna się od daty podpisania protokołu odbioru końcowego. 3. Serwis gwarancyjny świadczony w miejscu instalacji sprzętu. 4. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) w ciągu 1dnia roboczego od momentu zgłoszenia usterki w trybie 8x5xNBD. 5. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. 6. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
6	Inne	1. Wykonawca dostarczy i zainstaluje urządzenie UTM we wskazanym miejscu w lokalizacji Zamawiającego, w siedzibie Centralnego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, ul. Jana Olbrachta 94, 01-102 Warszawa. 2. Dostarczony sprzęt musi być fabrycznie nowy i oryginalnie zapakowany. 3. Wykonawca przeprowadzi wdrożenie dostarczonego urządzenia UTM zastępując nim obecnie pracujące urządzenie UTM Zamawiającego (FortiGate 800A). Konfiguracja obecnego urządzenia UTM składa się z następujących elementów: *150 – polityk* *350 - obiektów adresowych firewalla* *60 obiektów firewall service custom* *90 – tuneli VPN* *Routing – tylko statyczny, 100 pozycji (90 do tuneli VPN)* 4. Wykonawca przeprowadzi szkolenie dla dwóch pracowników Zamawiającego z konfiguracji urządzenia z zakresu wdrożenia. 5. Wykonawca zapewni, dla jednej osoby, autoryzowane przez producenta dostarczonego urządzenia UTM, szkolenie z zakresu konfiguracji podstawowych oraz zaawansowanych funkcjonalności dostępnych w dostarczonym urządzeniu UTM. Wraz ze szkoleniem Wykonawca dostarczy bezpłatny Voucher, ważny przez minimum 3 miesiące (począwszy od daty ukończenia szkolenia) na egzamin certyfikujący (certyfikat producenta dostarczonego urządzenia UTM) potwierdzający zdobyte podczas szkolenia

		umiejętności. Szkolenie będzie realizowane na terenie Polski, prowadzone w języku polskim, materiały szkoleniowe mogą być w języku polskim lub angielskim. Zamawiający pokrywa koszty dojazdu oraz koszty zakwaterowania osoby objętej szkoleniem.

2. Router – 1 szt.

Tabela 2 Minimalne, wymagane parametry techniczne pojedynczego routera.

Lp	Nazwa	Parametry minimalne
1	Architektura	1. Urządzenie powinno pełnić rolę wielousługowego routera modularnego. 2. Możliwość instalacji co najmniej: a. 3 kart sieciowych z interfejsami, b. 2 modułów usługowych z interfejsami lub 5 modułów ogólnego przeznaczenia do dowolnego wykorzystania. Moduły usługowe powinny mieć możliwość wyłączania ich w celu oszczędzania energii. c. 1 wewnętrznego modułu DSP (architektura urządzenia powinna dopuszczać możliwość stosowania kart rozszerzeń z dodatkowymi, wbudowanymi modułami DSP) 3. Zainstalowany wewnętrzny, sprzętowy moduł akceleracji szyfrowania. 4. Możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora. 5. Posiada wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. 6. Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy muszą mieć możliwość obsadzenia modułami: a. z co najmniej sześcioma portami Gigabit Ethernet (z interfejsami miedzianymi i możliwością instalacji wkładek optycznych SFP) b. z co najmniej czterema portami Gigabit Ethernet (z interfejsami miedzianymi i możliwością instalacji wkładek optycznych SFP), które mogą być stosowane zamiennie z portem 10 Gigabit Ethernet, c. przełącznika Ethernet (funkcje L2 i L3) o całkowitej ilość portów nie mniejszej niż 48 (moduły przełącznika muszą być dostępne również w wersji z zasilaniem PoE), 7. Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową muszą mieć możliwość obsadzenia kartami: a. z portami szeregowymi o gęstości co najmniej 4 porty na moduł, b. z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł, 4 portów per moduł oraz 8 portów per moduł, c. umożliwiającymi instalację dysków SSD (minimum dla jednego slotu) 8. Slot urządzenia przewidziany pod rozbudowę o moduł z układami DSP musi mieć możliwość obsadzenia modułem: a. o gęstości nie mniejszej niż 256 kanałów, b. pozwalającym na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing), 9. Urządzenie musi oferować wydajność co najmniej 2Gbps.
2	Oprogramowanie, funkcjonalność	1. Obsługa protokołów routingu IPv4 takich, jak RIPv2, OSPF, BGPv4, OSPF, ISIS, EIGRP, a także routingu statycznego. 2. Obsługa protokołów routingu IPv6 takich, jak RIPng, OSPFv3, BGPv4, ISIS, EIGRP, a także routingu statycznego. 3. Obsługa protokołów routingu multicastowego PIM Sparse oraz PIM SSM, a także oraz routingu statycznego.

		4. Protokół BGP musi posiadać obsługę 4 bajtowych ASN. 5. Wsparcie dla funkcjonalności Policy Based Routing. 6. Obsługa mechanizmu Unicast Reverse Path Forwarding (uRPF). 7. Obsługa tzw. routingu między sieciami VLAN w oparciu o trunking 802.1Q. 8. Obsługa IPv6 w tym ICMP dla IPv6 oraz protokołów routingu IPv6 takich jak EIGRP, RIP, OSPFv3, IS-IS, 9. Obsługa list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL. 10. Obsługa NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast. 11. Wsparcie dla protokołów WCCP i WCCPv2. 12. Obsługa mechanizmu DiffServ. 13. Możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu. 14. Obsługa mechanizmów kolejkowania ruchu: a. z obsługą kolejki absolutnego priorytetu, b. ze statyczną alokacją pasma dla typu ruchu, c. WFQ. 15. Obsługa mechanizmu WRED. 16. Obsługa protokołu GRE oraz mechanizm honorowania IP Precendence dla ruchu tunelowanego. 17. Obsługa protokołu NTP. 18. Obsługa DHCP w zakresie Client , Server. 19. Obsługa tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika). 20. Obsługa mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+. 21. Funkcjonalność pozwalająca na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Monitor – EEM, lub odpowiednik). 22. Funkcjonalność EEM musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych. 23. Funkcjonalność EEM musi pozwalać na generowanie akcji takich jak: a. wykonanie komendy z poziomu linii poleceń urządzenia, b. wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej, c. wykonanie skryptu, d. wygenerowanie SNMP trap, e. ustawienie lub modyfikacja określonego licznika systemowego. 24. Funkcjonalność automatycznej optymalizacji routingu dla połączeń typu multihomed (funkcjonalność Optimized Edge Routing lub odpowiednik). 25. Funkcjonalność OER (lub odpowiednik) musi posiadać wsparcie dla: a. optymalizacji ruchu przychodzącego z wykorzystaniem rozgłaszania informacji BGP do zewnętrznych routerów (BGP external peers), b. optymalizacji ruchu głosowego, c. optymalizacji w oparciu o informację z protokołów warstw wyższych (protokoły i porty UDP/TCP), d. optymalizacji ruchu dla tuneli VPN IPSec/GRE, e. optymalizacji ruchu w oparciu o automatyczne wykrywanie ruchu aplikacyjnego. 26. Wsparcie dla Layer-2 Tunneling Protocol Version 3. 27. Wsparcie dla następujących funkcjonalności bezpieczeństwa sieciowego: a. funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES/AES, b. algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:

		i. Elliptic Curve Diffie-Hellman (ECDH), ii. Galois Counter Mode Advanced Encryption Standard (GCM-AES) 128/256 bitów, iii. Galois Message Authentication Code (GMAC-AES) 128/256 bitów, iv. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2, c. możliwość konfiguracji tuneli IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2). Wsparcie dla IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych, dla ruchu IPv4 oraz IPv6, z obsługą ruchu szyfrowanego z wydajnością co najmniej 85Mbps, d. funkcjonalność VPN musi wspierać tworzenie niezależnych VPN (w tym różnego typu: site-2-site, dynamicznych), e. technologia umożliwiająca szyfrowanie IPSec ruchu unicast IPv4 bez konieczności tworzenia tuneli, z użyciem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547, w tym: i. mechanizm pasywnego IPSec SA, w którym urządzenie akceptuje zaszyfrowany i niezaszyfrowany ruch przychodzący, ale wysyła zawsze ruch zaszyfrowany, ii. mechanizm fail-close, w którym urządzenie nie wysyła ruchu, w sytuacji kiedy miałby on pozostać niezaszyfrowany w przypadku kiedy urządzenie jest niezarejestrowane w sieci VPN, iii. mechanizm współdzielenia kluczy przez redundantne serwery kluczy, iv. mechanizm zmiany podstawowego serwera kluczy (Key Server) w scenariuszu z wysoką dostępnością serwerów kluczy, f. funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall), g. funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall), h. możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, w tym: i. przesyłu, który jest poddawany inspekcji, ii. przesyłu, który jest odrzucany, iii. przesyłu, który jest przenoszony bez inspekcji, i. ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU, j. możliwość logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU, k. możliwość wymuszenia reguł złożoności haseł tworzonych na urządzeniu, l. w przypadku modułu przełącznika, działającego jako urządzenie dostępowe RADIUS (NAD - Network Access Devices), wsparcie funkcjonalności 802.1x. 28. Możliwość rozbudowy do następujących funkcjonalności poprzez zakup odpowiednich licencji i opcji sprzętowych: a. funkcjonalność procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia) dla co najmniej 450 abonentów, b. funkcje pozwalające na automatyzację konfiguracji ustawień QoS (w szczególności dla usług VoIP) w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS, c. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez

		symulację kodeków VoIP i mierzenie parametrów opóźnienia "tam i z powrotem" (roundtrip, jitter i utraty pakietów), d. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych, przy czym brama taka musi mieć możliwość pracy w sposób niezależny lub być sterowana przez system centralny procesowania połączeń.
3	Zarządzanie i konfiguracja	1. Zarządzanie za pomocą SNMPv1, SNMPv2, SNMPv3, Telnet, SSH. 2. Możliwość eksportu statystyk ruchowych za pomocą protokołu Neftflow/JFlow lub odpowiednika. 3. Konfigurowanie za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI). 4. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
4	Obudowa	1. Wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej. 2. Możliwość montażu w szafie 19”. Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19”, jeśli nie są one integralną częścią urządzenia
5	Zasilanie	1. Urządzenie musi być wyposażone w minimum 2 redundantne zasilacze zmienno-prądowe AC 230V. 2. Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia (funkcja wymagana).
6	Wyposażenie	1. Urządzenie musi być wyposażone w minimum 4 interfejsy Gigabit Ethernet 10/100/1000 RJ45 dla realizacji połączenia do sieci LAN. Wszystkie interfejsy muszą mieć możliwość pracy z gigabitowym portem światłowodowym definiowanym przez wkładki GBIC, SFP lub równoważne. Porty wyposażone we wkładki światłowodowe (4 szt.) umożliwiające komunikację światłowodową z innymi urządzeniami Zamawiającego (switche i router firmy Cisco) wyposażonymi we wkładki typu GLC-SX-MM. 2. 2 szt. patchcordów światłowodowych o długości 3 m oraz 2 szt. o długości 5m, typu LC-LC, kompatybilnych z dostarczonymi wkładkami światłowodowymi oraz wkładkami GLC-SX-MM posiadanymi przez Zamawiającego. 3. Dodatkowo urządzenie musi być wyposażone w moduł przełącznika L2 z minimum 4 interfejsami Gigabit Ethernet 10/100/1000 RJ45. 4. Urządzenie musi być wyposażone w minimum 16GB pamięci Flash. 5. Urządzenie musi być wyposażone w minimum 16GB pamięci RAM. 6. Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych. 7. Wszystkie karty i moduły muszą być objęte wspólnym serwisem producenta.
7	Gwarancja	1. Gwarancja na bazie świadczenia gwarancyjnego producenta sprzętu przez okres minimum 36 miesięcy. Wykonawca zapewnia, że dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji producenta sprzętu. Z dostawą sprzętu Wykonawca zobowiązuje się dostarczyć dokument wydany przez producenta lub jego polskiego przedstawiciela, potwierdzający że sprzęt jest nowy (potwierdzająca data produkcji), pochodzi z oficjalnego kanału dystrybucji, pochodzi z bieżącej produkcji i objęty jest

		wsparciem serwisowym producenta przez okres wymagany w SIWZ. 2. Okres gwarancji rozpoczyna się od daty podpisania protokołu odbioru końcowego. 3. Serwis gwarancyjny świadczony w miejscu instalacji sprzętu. 4. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 4 godzin. 5. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) w ciągu 1dnia roboczego od momentu zgłoszenia usterki w trybie 8x5xNBD. 6. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. 7. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
8	Inne	1. Wykonawca dostarczy i zainstaluje router we wskazanym miejscu w lokalizacji Zamawiającego, w siedzibie Centralnego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, ul. Jana Olbrachta 94, 01-102 Warszawa. 2. Dostarczony sprzęt musi być fabrycznie nowy i oryginalnie zapakowany. 3. Wykonawca przeprowadzi wdrożenie dostarczonego routera zastępując nim obecnie pracujący router Zamawiającego (Cisco 3845). Konfiguracja obecnego routera składa się z następujących elementów: 10 interfejsów / subinterfejsów *Routing – BGP* 1 peer 1 interfejs BGP do publicznego Internetu *Routing – EIGRP:* 2 interfejsy *Routing statyczny* 5 pozycji routingu statycznego *ACLs* 4 ACLs Średnio po 11 pozycji w ACLach *Prafix-lists* 1 prefix-list *Route-maps* 2 route-maps 4. Wykonawca przeprowadzi szkolenie dla dwóch pracowników Zamawiającego z konfiguracji urządzenia z zakresu wdrożenia. 5. Wykonawca dostarczy bezpłatny Voucher (dla jednej osoby), ważny przez okres minimum 24 miesiące (począwszy od daty odbioru zamówienia) na komplet egzaminów certyfikujących do stopnia Professional lub równoważny (certyfikat producenta dostarczonego routera) z zakresu zarządzania sieciami komputerowymi opartymi o routery i switche. Egzaminy będą się odbywać na terenie Polski w języku polskim lub angielskim.

3. Przełącznik – 2 szt.

Tabela 3 Minimalne, wymagane parametry techniczne pojedynczego przełącznika.

Lp	Nazwa	Parametry minimalne
1	Rodzaj urządzenia	1. Przełącznik wyposażony w minimum 48 portów 10/100/1000BaseT oraz 4 porty uplink 1/10Gigabit Ethernet SFP+ 2. Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10GE – minimum 10GBase-SR, LR, LRM, ER i twinax oraz Gigabit Ethernet – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U, EX, ZX oraz modułami CWDM zależnie od potrzeb.
2	Architektura	1. Przełącznik musi zapewniać możliwość rozbudowy o możliwość łączenia w stos z zapewnieniem następujących parametrów: a. Przepustowość w ramach stosu min. 160Gb/s b. Min. 9 urządzeń w stosie c. Zarządzanie poprzez jeden adres IP d. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad 2. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów 3. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego wymagania. Zasilacze muszą być wymienne 4. Obsługa standardu IEEE 802.3az Energy-Efficient Ethernet (EEE) 5. Możliwość instalacji zasilacza prądu stałego 6. Możliwość rozszerzenia funkcjonalności o funkcję kontrolera sieci bezprzewodowej WiFi (poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych) z zachowaniem następujących parametrów: a. Centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM) b. Przepustowość dla sieci WiFi nie mniejsza niż 40Gb/s c. Obsługa minimim 25 punktów dostępowych d. Obsługa minimum 1000 klientów sieci WiFi e. Możliwość terminowania tuneli CAPWAP na przełączniku f. Elastyczne mechanizmy QoS dla sieci WiFi w tym możliwość definiowania parametrów usług per punkt dostępowy/SSID/klient sieci WiFi g. Zarządzanie pasmem radiowym punktów dostępowych: i. automatyczna adaptacja do zmian w czasie rzeczywistym ii. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia) iii. dynamiczne przydzielanie kanałów radiowych iv. wykrywanie, eliminacja i unikanie interferencji v. równoważenie obciążenia punktów dostępowych vi. automatyczna dystrybucja klientów pomiędzy punkty dostępowe vii. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych h. Mapowanie SSID do segmentów VLAN w sieci przewodowej i. 1:1 ii. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty) iii. tunelowanie ruchu klientów do przełącznika/kontrolera

		i. Obsługa mechanizmów bezpieczeństwa: i. 802.11i, WPA2, WPA ii. 802.1X z EAP (PEAP, EAP-TLS, EAP-FAST) iii. możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID iv. możliwość profilowania użytkowników: 1. przydział sieci VLAN 2. przydział list kontroli dostępu (ACL) v. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509 vi. obsługa list kontroli dostępu (ACL) vii. ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników j. Obsługa ruchu unicast i multicast IPv4: i. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym) ii. obsługa konwersji ruchu multicast do unicast k. Obsługa mobilności (roamingu) użytkowników (L2 i L3) l. Obsługa mechanizmów QoS: i. 802.1p, WMM, TSpec ii. ograniczanie pasma per użytkownik iii. Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu iv. U-APSD m. Obsługa dostępu gościnnego: i. przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony) ii. możliwość kreowania użytkowników z określeniem czasu ważności konta n. Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne oraz usługi bezpieczeństwa o. Możliwość analizy ruchu pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji w warstwie 7
3	Wydajność	1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) 2. Minimum 4GB pamięci DRAM i 2GB pamięci flash 3. Obsługa minimum: a. 4.000 sieci VLAN b. 32.000 adresów MAC c. 24.000 tras IPv4
4	Oprogramowanie/ funkcjonalność	1. Obsługa protokołu NTP 2. Obsługa IGMPv1/2/3 3. Wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci: a. IEEE 802.1w Rapid Spanning Tree b. IEEE 802.1s Multi-Instance Spanning Tree c. Obsługa minimum 128 instancji protokołu STP 4. Obsługa protokołu LLDP i LLDP-MED 5. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego 6. Możliwość uruchomienia funkcji serwera DHCP

		7. Wsparcie dla następujących mechanizmów związanych z zapewnieniem bezpieczeństwa sieci: a. Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level) b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 i. Minimum 3000 wpisów dla list kontroli dostępu (ACE) j. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www) k. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard l. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) m. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+ n. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia) 8. Wsparcie dla następujących mechanizmów związanych z zapewnieniem jakości usług w sieci: a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi b. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP e. Możliwość ograniczania pasma dostępnego na danym porcie dla ru-

		chu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik f. Kontrola sztormów dla ruchu broadcast/multicast/unicast g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP 9. Wbudowane reflektometry (TDR) dla portów 10/100/1000 10. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych 11. Obsługa protokołu HSRP/VRRP lub mechanizmu równoważnego dla usług redundancji bramy
5	Zarządzanie i konfiguracja	1. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN) 2. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 48 000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow 3. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) 4. Dedykowany port Ethernet do zarządzania out-of-band 5. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB 6. Urządzenie musi być wyposażone w port konsoli USB 7. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją 8. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie 9. Urządzenie musi posiadać wbudowany analizator pakietów 10. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
6	Obudowa	1. Możliwość montażu w szafie 19”. Urządzenie będzie dostarczone wraz z elementami montażowymi do szafy RACK 19”, jeśli nie są one integralną częścią urządzenia 2. Wysokość urządzenia nie maksymalnie 1 RU
7	Wyposażenie	1. Oferowany przełącznik musi być wyposażony w:

		a. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy b. Moduł stakujący wraz z kablem o długości 3m 2. 4 szt. modułów światłowodowych Gigabit Ethernet, umożliwiających komunikację światłowodową z innymi urządzeniami Zamawiającego (switche i router firmy Cisco) wyposażonymi we wkładki typu GLC-SX-MM. 3. 4 szt. patchcordów światłowodowych LC-LC o długości 1,5m, kompatybilnych z dostarczonymi wkładkami światłowodowymi oraz wkładkami GLC-SX-MM posiadanymi przez Zamawiającego. 4. Wymagane jest, aby moduły SFP/SFP+ oferowane wraz z urządzeniem pochodziły od tego samego producenta co przełącznik celem uniknięcia problemów z serwisowaniem urządzeń
8	Gwarancja	1. Gwarancja na bazie świadczenia gwarancyjnego producenta sprzętu przez okres minimum 36 miesięcy. Wykonawca zapewnia, że dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji producenta sprzętu. Z dostawą sprzętu Wykonawca zobowiązuje się dostarczyć dokument wydany przez producenta lub jego polskiego przedstawiciela, potwierdzający że sprzęt jest nowy (potwierdzająca data produkcji), pochodzi z oficjalnego kanału dystrybucji, pochodzi z bieżącej produkcji i objęty jest wsparciem serwisowym producenta przez okres wymagany w SIWZ. 2. Okres gwarancji rozpoczyna się od daty podpisania protokołu odbioru końcowego. 3. Serwis gwarancyjny świadczony w miejscu instalacji sprzętu. 4. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 4 godzin. 5. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) w ciągu 1dnia roboczego od momentu zgłoszenia usterki w trybie 8x5xNBD. 6. Serwis gwarancyjny świadczony przez 8 godzin na dobę przez 5 dni w tygodniu od poniedziałku do piątku. 7. Przyjmowanie zgłoszeń serwisowych od Zamawiającego odbywać się powinno przez telefon (przez 8 godzin dziennie w przedziale godzinowym od 7:00 do 17:00), fax, e-mail lub WWW (przez całą dobę). Wykonawca przekaże Zamawiającemu dane kontaktowe do punktu przyjmowania zgłoszeń serwisowych w Polsce. Przyjmowanie zgłoszeń odbywać się musi w języku polskim.
9	Inne	1. Wykonawca dostarczy i zainstaluje przełączniki we wskazanym miejscu w lokalizacji Zamawiającego, w siedzibie Centralnego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, ul. Jana Olbrachta 94, 01-102 Warszawa. 2. Dostarczony sprzęt musi być fabrycznie nowy i oryginalnie zapakowany. 3. Wykonawca przeprowadzi wdrożenie dostarczonych przełączników zastępując nimi obecnie pracujące przełączniki Zamawiającego (Cisco 3560 i Cisco 2960). Konfiguracja obecnych przełączników składają się z następujących elementów: *8 sieci VLAN* *brak routingu, tylko przełączanie warstwy 2.* 4. Wykonawca przeprowadzi szkolenie dla dwóch pracowników Zamawiającego z konfiguracji urządzeń z zakresu wdrożenia.