Postępowanie nr 13/ROUTERY/2023
Załącznik nr 1 do SWZ
Załącznik nr 1 do umowy

Opis przedmiotu zamówienia
Zakup routerów brzegowych (część nr 1),
przełączników sieciowych i punktów dostępowych (część 2).

Postępowanie podzielone jest na dwie części

część I - Zakup 12 sztuk Routerów brzegowych/PaloAlto PA-440
część II – Zakup przełączników sieciowych (ilość szt. 3) oraz punktów dostępowych (ilość szt. 15)

Główny kod CPV: 3242000-3 – urządzenia sieciowe

<u>część I - Zakup 12 sztuk Routerów PaloAlto PA-440 z licencjami premium partner support oraz 11 licencji premium partner support do posiadanych urządzeń PA-440.</u>

Urządzenie PaloAlto w pełni kompatybilne z urządzeniem PaloAlto PA-850 zainstalowanym w siedzibie głównej zamawiającego, spełniające następujące parametry techniczne:

Lp.	Opis wymaganego parametru
1	Zamawiający wymaga, aby zaoferowane urządzenia były uznanymi rozwiązaniami na świecie – producent zaoferowanego rozwiązania musi być notowany w raportach Gartnera dla rozwiązań Enterprise Network Firewall nie starszych niż 2 lata przed złożeniem oferty. Jako równoważny dla raportu Gartnera Zamawiający dopuści również inny raport udostępniany publicznie, powszechnie akceptowany, mający charakter zewnętrznego i obiektywnego raportu standaryzacyjnego, który zapewnia analizę, wgląd w kierunek oraz dojrzałość uczestników rynku w rozwiązaniach typu Network Firewall, aktualizowany co roku od min. 20 lat.
2	Klasa urządzenia: specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybie Active/Standby.
3	Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent ferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat.
4	Urządzenia muszą umożliwiać działanie w następujących trybach pracy: a. rutera (tzn. w warstwie 3 modelu OSI), b. mostu (tzn. w warstwie 2 modelu OSI), c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.). d. w trybie pasywnego nasłuchu (sniffer/tap).
5	System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
6	Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 oraz w co najmniej jeden dedykowany port ethernet 10/100/1000 na cele zarządzania out-of-band.
7	Urządzenia firewall muszą posiadać logiczną separację zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
8	Urządzenia firewall muszą posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
9	Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być

	tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
10.	Urządzenia firewall muszą wspierać protokół LACP.
11.	Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
12.	Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
13.	Polityka zabezpieczeń firewall musi uwzględniać a. adresy IP źródłowe i docelowe, b. protokoły i usługi sieciowe, c. aplikacje, d. kategorie URL, e. użytkowników aplikacji i grupy, f. reakcje zabezpieczeń, g. logowanie zdarzeń (początek i koniec sesji) h. strefa wejściowa i wyjściowa
14.	Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
15.	Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
16.	Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
17.	Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
18.	Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
19.	Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
20.	Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami: a. Active Directory, b. Terminal Services c. Syslog
21.	Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
22.	Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
23.	Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania

	raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
24.	Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykietami musi pozwalać na użycie: a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia) b. API
25.	Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
26	Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF dla IPv4 i IPv6.
27.	Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
28.	Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
29.	Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
30.	Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.
31.	Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
32.	Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
33.	Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
34.	Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
35.	Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
36.	Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
37.	Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
38.	Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
39.	Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
40.	Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell).
41.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (IPS). Baza sygnatur takiego modułu musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. W obecnym postepowaniu licencja nie jest wymagana.
42.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół

	minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 24 godziny i pochodzić od tego samego producenta co firewall. W obecnym postepowaniu licencja nie jest wymagana.
43.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall. W obecnym postepowaniu licencja nie jest wymagana.
44.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję filtrowania URL w oparciu o kategorie związane z treścią oraz poziomem ryzyka. Baza kategorii URL musi pochodzić od tego samego producenta. W obecnym postepowaniu licencja nie jest wymagana.
45.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję przechwytywania i przesyłania do zewnętrznego systemu sandbox plików wykonywalnych PE, DLL, ELF oraz JAR przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. W obecnym postepowaniu licencja nie jest wymagana.
46.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o ochronę DNS w zakresie: a. możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing), b. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA), c. wykrywanie domen dynamicznych Dynamic DNS, d. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych. W obecnym postepowaniu licencja nie jest wymagana.
47.	Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz co najmniej dla 1000 użytkowników. Oprogramowanie klienta Remote Access VPN musi pochodzić od tego samego producenta i być objęte wsparciem technicznym producenta w takim samym okresie jak okres wsparcia technicznego, którym będzie objęty firewall.
48.	Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
49.	W przypadku gdy jakakolwiek funkcjonalność (włącznie z klientem Remote Access VPN) lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 12 miesięcy od daty odbioru sprzętu.
50.	Wsparcie serwisowe (techniczne) i gwarancja dla systemu (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 12 miesięcy od daty odbioru sprzętu.
51.	Urządzenie musi być wyposażone w minimum: a. 8 wbudowanych interfejsów 10/100/1000 Ethernet (RJ45)
52.	Urządzenie musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 120 GB na potrzeby systemu operacyjnego, logów i rejestrowania pakietów.
53.	Urządzenie musi być wyposażone w co najmniej dwa zasilacze AC.
54.	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: a. Minimum 2,4 Gbps dla rozpoznawania i kontroli aplikacji, b. Minimum 1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych co najmniej następujących funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików i z włączonym logowaniem na dysk urządzenia. Funkcje bezpieczeństwa muszą być skonfigurowane w trybie

	gwarantującym najwyższy poziom ochrony (włączone wszystkie sygnatury IPS i wszystkie sygnatury AV) c. Minimum 39 000 nowych sesji na sekundę. d. Minimum 200 000 równoległych sesji
55.	Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.
56.	Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 2000 reguł polityki bezpieczeństwa.

część II – Zakup przełączników sieciowych z modułami stackującymi i licencjami (ilość szt. 3) oraz punktów dostępowych z licencjami (ilość szt. 15)

a) Przełączniki sieciowe

Parametry minimalne

1. Typ i liczba portów:
   48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP
3. Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
   3.1. Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
   3.2. Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
4. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
   4.1. Przepustowość w ramach stosu - 80Gb/s
   4.2. 8 urządzeń w stosie
   4.3. Zarządzanie poprzez jeden adres IP
   4.4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5. Zasilanie i chłodzenie
   5.1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
   5.3. Redundantne wentylatory
6. Parametry wydajnościowe:
   6.1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
   6.2. Bufor pakietów – 6MB
   6.3. Pamięć DRAM – 2GB
   6.4. Pamięć flash – 4GB
   6.5. Obsługa
      6.5.1.1000 sieci VLAN
      6.5.2.16.000 adresów MAC
      6.5.3.3.000 tras IPv4
      6.5.4.1.500 tras IPv6
7. Obsługa protokołu NTP
8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   9.1. IEEE 802.1w Rapid Spanning Tree
   9.2. Per-VLAN Rapid Spanning Tree (PVRST+)
   9.3. IEEE 802.1s Multi-Instance Spanning Tree
   9.4. Obsługa 64 instancji protokołu STP
10. Obsługa protokołu LLDP i LLDP-MED.
11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
12. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
13. Możliwość uruchomienia funkcji serwera DHCP

14. Mechanizmy związane z bezpieczeństwem sieci:
    14.1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    14.2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    14.3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    14.4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    14.5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    14.6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    14.7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
    14.8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
    14.9. 1500 wpisów dla list kontroli dostępu (Security ACE)
    14.10. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)
    14.11. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    14.12. 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)
    14.13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
    14.14. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
    14.15. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host)
    14.16. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)
    14.17. Funkcja Private VLAN
15. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
    16.1 Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne, jednoukładowe rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
    16.2 Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
    16.3 .Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.
16. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    16.1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    16.2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
    16.3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    16.4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    16.5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)
    16.6. Kontrola sztormów dla ruchu broadcast/multicast/unicast
    16.7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
17. Obsługa protokołów routingu:
    17.1. Routing statyczny dla IPv4 i IPv6

17.2. Routing dynamiczny – RIP, OSPF
17.3. Policy-based routing (PBR)
17.4. Obsługa protokołu redundancji bramy (VRRP)

18. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
19. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
20. Możliwość uruchamiania skryptów Python poprzez Embedded Event Manager
21. Zarządzanie
    21.1. Port konsoli
    21.2. Dedykowany port Ethernet do zarządzania out-of-band
    21.3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
    21.4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
    21.5. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
    21.6. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych
    21.7. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą
    21.8. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
22. Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
26. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 16.000 strumieni
27. Wbudowany analizator pakietów

b) Punkty dostępowe
Parametry minimalne

Autentykacja i bezpieczeństwo	● Wi-Fi Protected Access - with WPA2 or WPA3, including WPA2-Entperprise authentication
	● 802.1X, RADIUS Authentication, Authorization, and Accounting (AAA)
	● Segmentation via VLANs (up to 16)
	● 802.11r and 802.11i
	● Guest network can also authenticate against a Social Login account: Google and Facebook
Maksymalna ilość klientów	● Maximum number of associated wireless clients: 200 per Wi-Fi radio, for a total of 400 clients per access point, or 1000 in a system
Zarządzanie	● Zarządzanie z centralnego systemu
802.11ax	● 2x2 downlink MU-MIMO with two spatial streams
	● Uplink/downlink OFDMA
	● TWT
	● BSS coloring
	● MRC
	● 802.11ax beamforming
	● 20-, 40-, 80- channels
	● PHY data rates up to 1.488 Gbps (80 MHz with 5 GHz and 20 MHz with 2.4 GHz)
	● Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive)
	● 802.11 DFS
	● CSD support

	● WPA3 support	
802.11ac	● 2x2 single-user/multi-user MIMO with two spatial streams, up to 867 Mbps in 5GHz	
	● 20-, 40-, and 80-MHz channels	
	● Dynamic Frequency Selection (DFS)	
Porty Ethernet	● Autentykacja 802.1X lub filtrowanie MAC	
	Dynamiczny VLAN dla portu	
	● Traffic locally switched or tunneled back to Master AP	
Przepustowość	802.11a: 6, 9, 12, 18, 24, 36, 48, i 54 Mbps	
	802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, i 54 Mbps	
	802.11n 2.4 GHz: 6.5 do 300 Mbps (MCS0-MCS15, HT 20/40)	
	802.11ac 5 GHz: 6.5 do 867 Mbps (MCS0-MCS9)	
	802.11ax 2.4 & 5GHz: 6.5 do 1200 Mbps (MCS0-MCS11)	
Zintegrowane anteny	2.4GHz: zysk szczytowy 4dBi, dookólna	
	5GHz: zysk szczytowy 5dBi, dookólna	
Maksymalna ilość nie nakładających się kanałów	A (A regulatory domain):	Q (Q regulatory domain):
	● 2.412 to 2.462 GHz; 11 channels	● 2.412 to 2.472 GHz; 13 channels
	● 5.180 to 5.320 GHz; 8 channels	● 5.180 to 5.320 GHz; 8 channels
	● 5.500 to 5.700 GHz; 8 channels	● 5.500 to 5.700 GHz; 11 channels
	◦ excludes 5.600 to 5.640 GHz	R (R regulatory domain):
	● 5.745 to 5.825 GHz; 5 channels	● 2.412 to 2.472 GHz; 13 channels
	B (B regulatory domain):	● 5.180 to 5.320 GHz; 8 channels
	● 2.412 to 2.462 GHz; 11 channels	● 5.660 to 5.700 GHz; 3 channels
	● 5.180 to 5.320 GHz; 8 channels	● 5.745 to 5.805 GHz; 4 channels
	● 5.500 to 5.720 GHz; 12 channels	Z (Z regulatory domain):
	● 5.745 to 5.825 GHz; 5 channels	● 2.412 to 2.462 GHz; 11 channels
	E (E regulatory domain):	● 5.180 to 5.320 GHz; 8 channels
	● 2.412 to 2.472 GHz; 13 channels	● 5.500 to 5.700 GHz; 8 channels
	● 5.180 to 5.320 GHz; 8 channels	◦ excludes 5.600 to 5.640 GHz
	● 5.500 to 5.700 GHz; 8 channels	● 5.745 to 5.825 GHz; 5 channels
	I (I regulatory domain):	
	● 2.412 to 2.472 GHz; 13 channels	
	● 5.180 to 5.320 GHz; 8 channels	
Dostępna moc nadajnika	2.4 GHz	5 GHz
	do 20 dBm	do 20 dBm
Interfejsy	● 1x Gigabit Ethernet (10/100/1000BASE-T auto negocjacja), Power over Ethernet (PoE)	

System	● 1 GB DRAM, 512MB flash
	● 1GHz quad core processor
Zasilanie	● Zasilanie z POE
	● IEEE standards:
	◦ IEEE 802.3
	◦ IEEE 802.3ab
	◦ IEEE 802.3af/at
	◦ IEEE 802.11a/b/g/n/ac/ax
	◦ IEEE 802.11h, 802.11d
	● Security:
	◦ 802.11i, WPA2, WAP3, WPA
	◦ 802.1X
	◦ AES
	● Extensible Authentication Protocol (EAP) types:
	◦ EAP-Transport Layer Security (TLS)
	◦ EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
	◦ Protected EAP (PEAP) v0 or EAP-MSCHAPv2
	◦ EAP-Flexible Authentication via Secure Tunneling (FAST)
	◦ PEAP v1 or EAP-Generic Token Card (GTC)
	◦ EAP-Subscriber Identity Module (SIM)
	● Multimedia:
	◦ Wi-Fi Multimedia (WMM)
	◦ RSS-102

<u>WYMAGANIA OGÓLNE</u>

W ramach realizacji Przedmiotu Zamówienia Wykonawca zobowiązany będzie do m.in.:
a) dostarczenia wszystkich urządzeń do siedziby zamawiającego na własny koszt i ryzyko,
b) zapewnienie wsparcia technicznego – serwisowego od momentu dostarczenia urządzeń przez okres 12 miesięcy.
c) zapewnienie dostępu do wszelkich aktualizacji i ich wdrożenie u Zamawiającego (możliwy zdalny suport),
d) wszelkie licencje powstałe w wyniku zakupionego sprzętu mają zostać wystawione na zamawiającego.

Termin realizacji zamówienia dla części 1 nie dłużej niż 12 tygodni na dostawę sprzętu od dnia podpisania umowy.

Termin realizacji zamówienia dla części 2 – w terminie zadeklarowanym przez Wykonawcę jako kryterium oceny ofert i nie może być dłuższy niż 28 dni.

Rozwiązania równoważne zaproponowane przez Wykonawcę mają zapewnić kompatybilność posiadanych urządzeń u Zamawiającego a w przypadku wprowadzenia nowszych technologicznie rozwiązań ciężar

udowodnienia równoważności oferowanego sprzętu z wymaganym przez Zmawiającego ciąży na Wykonawcy w tym również wszelkie inne nowe powstałe koszty.
W przypadku uszkodzenia urządzenia nie wynikającego z winy Kupującego lub jego awarii Wykonawca zapewni w jego miejsce nowego urządzenia wolne od wad .

Zamawiający wymaga aby **miał pełne prawa** do korzystania z licencji i oprogramowania zainstalowanego w urządzeniach

Zamawiający wymaga aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe były fabrycznie nowe i na dzień składania ofert niewycofane przez producenta ze sprzedaży

Zamawiający wymaga aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe pochodziły z **oficjalnego kanału dystrybucyjnego producenta urządzeń na rynek polski**

Zamawiający wymaga aby dostarczony sprzęt był **zarejestrowany na Krakowskie Pogotowie Ratunkowe lub jednostkę nadrzędną** w celu posiadania pełnych praw licencyjnych i gwarancyjnych

Zamawiający wymaga aby wszystkie dostarczane urządzenia posiadały **cechy/atrybuty ich legalności**, tj. oznaczenie producenta, modelu oraz numeru seryjnego urządzenia

Zamawiający wymaga aby Wykonawca przed dostawą (najpóźniej w dniu dostawy) dostarczył **numery seryjne urządzeń celem weryfikacji źródła** ich pochodzenia u producenta.
W przypadku negatywnej weryfikacji, Zamawiający może odmówić przyjęcia urządzeń.