Nr postępowania: OSO.271.13.2022

Załącznik nr 2a
do Specyfikacji Warunków Zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA
(zwany również „OPZ")

Dotyczy zamówienia pn.
Zakup komputerów i sprzętu biurowego w ramach projektu grantowego Cyfrowa Gmina
w zakresie części pierwszej – zadania nr 1 o nazwie
Zakup urządzeń typu firewall (UTM) oraz przełączników sieciowych realizowany w ramach projektu grantowego „Cyfrowa Gmina"

Dotyczy zamówienia pn. Zakup urządzeń typu firewall (UTM) oraz przełączników sieciowych realizowany w ramach projektu grantowego „Cyfrowa Gmina".

Wymagania dla zamówienia:

1. gwarancja na UTM'y musi być w postaci gwarancji producenta i gwarancją wykonawcy z naprawą w formie „od drzwi do drzwi" po konsultacji telefonicznej zamawiającego z producentem lub wykonawcą na okres wskazany w ofercie jednak nie krótszy niż 36 miesięcy. W momencie dostarczenia UTM'ów po uruchomieniu i zalogowaniu do urządzenia musi ono potwierdzać okres udzielonej gwarancji oraz informacje o wykupionych usługach każdego egzemplarza urządzenia. Okres gwarancji UTM'ów stanowi kryterium oceny ofert. Warunki gwarancji określa § 9 wzoru umowy w sprawie zamówienia publicznego;

2. gwarancja na przełączniki sieciowe musi być w postaci gwarancji producenta i gwarancją wykonawcy na okres 36 miesięcy z naprawą w formie „od drzwi do drzwi" po konsultacji telefonicznej zamawiającego z producentem lub wykonawcą. Warunki gwarancji określa § 9 wzoru umowy w sprawie zamówienia publicznego;
3. każdy dostarczany UTM oraz przełącznik sieciowy musi posiadać oznaczenia umieszczone w sposób trwały na każdym egzemplarzu sprzętu:
    a. numer seryjny nadany przez producenta,
    b. oznaczenie producenta,
    c. oznaczenie „CE" potwierdzające spełnienie wymogów dyrektywy tzw. „Nowego Podejścia" Unii Europejskiej;
4. W ramach zamówienia Wykonawca przeprowadzi szkolenie w formie webinarium z obsługi UTM'ów dla minimum 1 osoby. Szkolenie musi obejmować różne scenariusze konfiguracyjne oraz pytania i odpowiedzi Zamawiającego do Wykonawcy z obsługi i funkcji UTM'ów.
5. O ile nie zaznaczono inaczej, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne

Tabela I

Urządzenie typu firewall(UTM) o minimalnych parametrach jak poniżej – 2 szt.			
Lp.	**Element**	**Minimalne wymagane parametry dla poszczególnych elementów firewalla(UTM'a)**	**Przedmiotowy środek dowodowy potwierdzający minimalne wymagane parametry wskazane w Kolumnie B dla danego elementu wymienionego w Kolumnie A**
	Kolumna A	**Kolumna B**	**Kolumna C**
I.	Wymagania ogólne	1. Dostarczone urządzenie typu firewall(UTM) musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.	Spełnienie wymagania dla elementu I. w kolumnie B w pkt. 1-5 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		2. System realizujący funkcję Firewall musi dawać możliwość pracy w co najmniej w trybach: routera z funkcją NAT lub transparentnym. 3. W ramach dostarczonego UTM'u musi być zapewniona możliwość budowy minimum 2 oddzielnych sieci fizycznych WAN, LAN oraz instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. 4. Musi istnieć możliwość dedykowania co najmniej dwóch administratorów do poszczególnych instancji systemów. 5. UTM musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji.	
II.	Złącza zewnętrzne i interfejsy	Dostarczony UTM musi posiadać: 6. Złącza ethernet 2 szt. WAN 10/100/1000. 7. Złącza ethernet 1 szt. DMZ. 8. Złącza ethernet 5szt. LAN 10/100/1000. 9. Złącze 1 szt. USB. 10. Złącze 1 szt. konsola(RJ45). 11. Zintegrowana obsługa sieci bezprzewodowej WiFi Single Radio (2.4GHz/5GHz), obsługa standardów 802.11 a/b/g/n/ac-W2.	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu II. w kolumnie B w pkt. 6-12 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie

		12. musi być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.	wymagań określonych dla elementu II. w kolumnie B w pkt. 6-12 OPZ.
III.	Dostarczone funkcje UTM'u	W ramach dostarczonego UTM'u muszą być realizowane wszystkie poniższe funkcje. 13. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 14. Kontrola Aplikacji. 15. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 16. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS. 17. Ochrona przed atakami - Intrusion Prevention System(IPS). 18. Kontrola stron WWW.	Spełnienie wymagania dla elementu III. w kolumnie B w pkt. 13-21 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		19. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 20. Zarządzanie pasmem (QoS, Trafficshaping). 21. Analiza ruchu szyfrowanego protokołem SSL.	
IV.	Parametry wydajnościowe	22. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 23. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 24. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 25. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 26. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) - minimum 1.4 Gbps. 27. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu IV. w kolumnie B w pkt. 22-28 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu IV. w kolumnie B w pkt. 22-28 OPZ.

		Control, Antywirus - minimum 700 Mbps. 28. Wydajność UTM'u w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.	
V.	Parametry modułu VPN	UTM musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 29. Wsparcie dla IKE v1 oraz v2. 30. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM). 31. Obsługa protokołu Diffie-Hellman grup 19 i 20. 32. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 33. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 34. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu V. w kolumnie B w pkt. 29-36 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu V. w kolumnie B w pkt. 29-36 OPZ.

		35. Obsługa mechanizmów: IPSec NAT Traversal, DPD. 36. Mechanizm „Split tunneling” dla połączeń Client-to-Site.	
VI.		UTM musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 37. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie UTM musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. 38. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 39. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie musi być zgodne z systemami Microsoft Windows 10 oraz Microsoft Windows 11. Oprogramowanie musi być nieogarnione czasowo oraz nieograniczone liczbą	Spełnienie wymagania dla elementu VI. w kolumnie B w pkt. 37-39 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		stanowisk komputerowych na których może być zainstalowane.	
VII.	Parametry modułu ochrony przed atakami	40. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 41. UTM powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 42. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 43. Administrator UTM'u musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 44. UTM musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 45. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym	Spełnienie wymagania dla elementu VII. w kolumnie B w pkt. 40-46 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		(co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 46. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
VIII.	Parametry modułu ochrony przed malware	47. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 48. UTM musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 49. UTM musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 50. UTM musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja	Spełnienie wymagania dla elementu VIII. w kolumnie B w pkt. 47-51 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		upoważniająca do korzystania z usługi typu Sandbox w chmurze. 51. UTM musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
IX.	Parametry modułu kontroli aplikacji	52. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 53. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 54. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 55. Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	Spełnienie wymagania dla elementu IX. w kolumnie B w pkt. 52-55 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		Administrator UTM'u musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
X	Parametry modułu kontroli WWW	56. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 57. W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 58. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 59. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 60. Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu X. w kolumnie B w pkt. 56-62 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu X. w kolumnie B w pkt. 56-62 OPZ.

		61. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 62. W ramach UTM'u musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - UTM nie będzie dokonywał inspekcji szyfrowanej komunikacji.	
XI.	Zarządzanie pasmem	63. UTM musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 64. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 65. UTM musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	Spełnienie wymagania dla elementu XI. w kolumnie B w pkt. 63-65 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.
XII.	Redundancja, monitoring i wykrywanie awarii	66. W przypadku UTM'u pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive.	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie

		W obu trybach musi istnieć funkcja synchronizacji sesji firewall. 67. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 68. Monitoring stanu realizowanych połączeń VPN. 69. UTM musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Musi istnieć możliwość tworzenia interfejsów redundantnych.	wymagań określonych dla elementu XII. w kolumnie B w pkt. 66-69 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu XII. w kolumnie B w pkt. 66-69 OPZ.
XIII.	Logowanie zdarzeń i ruchu	70. W ramach logowania UTM musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy UTM'u. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 71. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego	Spełnienie wymagania dla elementu XIII. w kolumnie B w pkt. 70-72 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		UTM'u. 72. Musi istnieć możliwość logowania zdarzeń na pamięć wewnętrzną SSD lub do serwera/usługi SYSLOG.	
XIV.	Zarządzanie urządzeniem	73. Elementy UTM'u muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i muszą mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 74. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 75. UTM musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 76. UTM musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	Spełnienie wymagania dla elementu XIV. w kolumnie B w pkt. 73-80 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		77. Urządzenie musi być wyposażone w graficzny interfejs umożliwiający konfigurację i obsługę urządzenia. 78. Graficzny interfejs musi umożliwiać wyświetlanie informacji o zakupionych licencjach(w tym okresu ich ważności) w oferowanym urządzeniu(dotyczy modułów: Antywirus, IPS, WWW). 79. Element UTM'u pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 80. UTM musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
XV.	Obudowa, pamięć i zasilanie	81. Obudowa urządzenia wolnostojąca z możliwością montażu uchwytów RACK. Uchwyty montażowe należy dostarczyć razem z urządzeniem. 82. Zewnętrzny zasilacz urządzenia 230V.	Spełnienie wymagania dla elementu XV. w kolumnie B w pkt. 81-83 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

		Zasilacz należy dostarczyć razem z urządzeniem. 83. Wbudowana pamięć SSD o pojemności 120GB.	
XVI.	Certyfikaty	84. Poszczególne elementy oferowanego UTM'u muszą posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.	Na potwierdzenie spełnienia wymagania dla elementu XVI. W kolumnie B w pkt. 84 należy dołączyć do oferty certyfikat ICSA lub EAL4 dla funkcji firewall w ramach oferowanego modelu UTM.
XVII.	Licencje	85. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Muszą one obejmować: Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres taki sam jak okres udzielonej gwarancji.	Spełnienie wymagania dla elementu XVII. w kolumnie B w pkt. 85 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.
XVIII.	Gwarancja i wsparcie	86. UTM musi być objęty serwisem gwarancyjnym producenta i wykonawcy przez okres 36 miesięcy**(kryterium oceny ofert)**., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. 87. W ramach serwisu gwarancyjnego	Spełnienie wymagania dla elementu XVIII. w kolumnie B w pkt. 86-87 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.

			producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie technicznego(telefonicznego oraz email).	

Tabela II.

Urządzenie sieciowe(przełącznik sieciowy –switch) o minimalnych parametrach jak poniżej – 2szt.			
Lp.	**Element**	**Minimalne wymagane parametry dla poszczególnych elementów przełącznika sieciowego**	**Przedmiotowy środek dowodowy potwierdzający minimalne wymagane parametry wskazane w Kolumnie B dla danego elementu wymienionego w Kolumnie A**
	Kolumna A	**Kolumna B**	**Kolumna C**
I.	Wymagania ogólne	1. Dostarczony przełącznik sieciowy(switch) musi być urządzeniem zarządzanym logicznie. 2. Switch musi w pełni współpracować z urządzeniem UTM opisanym tabeli „I" i dostarczonym w ramach tego Zamówienia.	Spełnienie wymagania dla elementu I. w kolumnie B w pkt. 1-2 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.
II.	Złącza zewnętrzne i interfejsy	Dostarczony switch musi posiadać: 3. Liczba podstawowych portów Ethernet: 24 4. Podstawowe porty Ethernet typu: Gigabit Ethernet (10/100/1000) 5. Liczba portów SPF: 2 6. Liczba portów konsoli RJ45: 1	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu II. w kolumnie B w pkt. 3-6 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie

			dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu II. w kolumnie B w pkt. 3-6 OPZ.
III.	Funkcje switcha	7. Dublowanie portów ethernet 8. Pełny dupleks transmisji 9. Podpora kontroli przepływu 10. Agregator połączenia 11. Kontrola wzrostu natężenia ruchu 12. Automatyczne MDI/MDI-X 13. Obsługa sieci VLAN. Funkcje wirtualnej sieci LAN Tagged VLAN. 14. Liczba VLANs 100. 15. Przekazywanie danych/pakietów metodą „Store-and-forward”	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu III. w kolumnie B w pkt. 7-15 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu III. w kolumnie B w pkt. 7-15 OPZ.
IV.	Pamięć przełącznika sieciowego	16. Pojemność pamięci wewnętrznej: 512 MB 17. Wielkość pamięci flash: 128 MB	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu IV. w kolumnie B w pkt. 16-17 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której

			znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu IV. w kolumnie B w pkt. 16-17 OPZ.
V.	Parametry wydajnościowe	18. Przepustowość przełączania: 56 Gbit/s 19. Wielkość tabeli adresów: 16000 wejścia	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu V. w kolumnie B w pkt. 18-19 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie wymagań określonych dla elementu V. w kolumnie B w pkt. 18-19 OPZ.
VI.	Standardy komunikacyjne	20. Obsługa standardów komunikacyjnych: IEEE 802.1D,IEEE 802.1Q,IEEE 802.1p,IEEE 802.1s,IEEE 802.1w,IEEE 802.1x,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ad,IEEE 802.3ae,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z	Na potwierdzenie spełnienia obok wskazanych minimalnych wymaganych parametrów należy: 1) złożyć wraz z ofertą dokument producenta (np. karta techniczna, specyfikacja) potwierdzający spełnienie wymagań określonych dla elementu VI. w kolumnie B w pkt. 20 OPZ, lub/i 2) wskazać wraz ze złożoną ofertą adres strony internetowej producenta (publicznie i powszechnie dostępnej bez konieczności logowania), na której znajdują się informacje potwierdzające spełnienie

			wymagań określonych dla elementu VI. w kolumnie B w pkt. 20 OPZ.
VII.	Zarządzanie urządzeniem	Możliwość zarządzania switchem przy pomocy protokołów/usług: 21. WWW-HTTP / HTTPS, 22. SNMP v1/v2c/v3, 23. SSH	Spełnienie wymagania dla elementu VII. w kolumnie B w pkt. 21-23 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.
VIII.	Obudowa, zasilanie	24. Obudowa switcha wolnostojąca z możliwością montażu uchwytów RACK. Uchwyty montażowe należy dostarczyć razem z urządzeniem. 25. Zewnętrzny zasilacz switcha 230V. Zasilacz należy dostarczyć razem ze switchem.	Spełnienie wymagania dla elementu VIII. w kolumnie B w pkt. 24-25 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.
IX.	Gwarancja i wsparcie	26. Przełączniki sieciowe muszą być objęte serwisem gwarancyjnym producenta i wykonawcy przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.	Spełnienie wymagania dla elementu IX. w kolumnie B w pkt. 26 OPZ zostanie zweryfikowane przez Zamawiającego podczas przeprowadzania odbioru jakościowego dostarczanego sprzętu.