

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa sprzętu sieciowego dla Powiatu Staszowskiego oraz odnowienia licencji urządzeń UTM dla jednostek podległych w ramach projektu „Cyberbezpieczny Samorząd”

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. Zamawiający jest w posiadaniu pewnych rozwiązań bezpieczeństwa producenta Fortinet. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymagany jest wymiana urządzenia Fortigate 100e będącego na stanie Zamawiającego wraz z usługą migracji, dostawa przełączników oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem.

Do oferowanych urządzeń poz. 1-5 razem z ofertą należy dołączyć następujące oświadczenia oraz certyfikaty (w języku polskim):

- Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej),
- Certyfikat ISO 9001 podmiotu serwisującego,
- oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
- W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
- Deklaracja zgodności CE
- RoHS/ROHS2

Wykonawca na dostarczony sprzęt udziela gwarancji na okres 12 miesięcy.

1. Wymiana urządzenia UTM w ramach programu Tradeup Fortigate 100E (FG100ETK19025813)na Fortigate 100F wraz z usługą migracji konfiguracji o cechach równoważności:

L.p	Parametry	Charakterystyka (wymagania minimalne)
1.	Wymagania ogólne	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.</p> <p>Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	<p>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system</p>

		<p>firewall zapewnia funkcję synchronizacji sesji.</p> <ol style="list-style-type: none"> Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie:	<ol style="list-style-type: none"> System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> 10 portami Gigabit Ethernet RJ-45. 8 gniazdami SFP 1 Gbps. 2 gniazdami SFP+ 10 Gbps. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	<ol style="list-style-type: none"> W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client

		<p>side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.5 Gbps.</p> <p>6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.</p> <p>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.</p>
5.	Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w

		<p>ramach połączeń VPN typu client-to-site.</p> <ol style="list-style-type: none"> Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Polityki, Firewall	<ol style="list-style-type: none"> Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> Translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

		<p>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <ul style="list-style-type: none"> • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
7.	Połączenia VPN	<p>1. System umożliwia konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

		<ul style="list-style-type: none"> • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
8.	Routing i obsługa łączności WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection).

		7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9.	Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
10.	Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub

		<p>umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <ol style="list-style-type: none"> System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
12.	Ochrona przed atakami	<ol style="list-style-type: none"> Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

		<ol style="list-style-type: none"> System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
13.	Kontrola aplikacji	<ol style="list-style-type: none"> Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są

		<p>kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <ol style="list-style-type: none"> 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
14.	Kontrola www	<ol style="list-style-type: none"> 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

		<ol style="list-style-type: none"> 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
16.	Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

		4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
14.	Zarządzanie	<ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

		<p>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
17.	Logowanie	<p>1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>4. Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>5. System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
18.	Testy wydajnościowe oraz funkcjonalne	<p>Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta.</p>

19.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów do 30.06.2026 roku. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen do 30.06.2026
20.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania do 30.06.2026 roku oraz wsparcie techniczne w trybie 24x7.
21.	Rozszerzone wsparcie serwisowe:	Hezo 360 lub równoważny: System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: <ul style="list-style-type: none"> • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.

		<ul style="list-style-type: none"> • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). • Przygotowanie urządzenia do zdalnej konfiguracji. • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. <p>Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</p> <p>Wymagania powinny być potwierdzone dokumentami:</p> <ul style="list-style-type: none"> • Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego
22.	Opisy do wymagań ogólnych	<p>1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania),</p>

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

2. Switch 48 portowy-5szt.

Lp.		
1.	Parametry fizyczne platformy	<ul style="list-style-type: none"> Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Maksymalny pobór mocy: 60 W. Minimalny zakres temperatury pracy: 0-40°C.

2.	Interfejsy sieciowe - wymagania minimalne	48 Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) porty GE RJ-45 b) 4 porty 10 GE SFP+.
3.	Zarządzanie	<ul style="list-style-type: none"> • Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
4.	Parametry wydajnościowe	Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. <ul style="list-style-type: none"> • Tablica adresów MAC o pojemności co najmniej 32k wpisów.

		<ul style="list-style-type: none"> Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
5.	Wymagane funkcje	<ul style="list-style-type: none"> Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. Obsługa Jumbo Frames. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). Agregacja portów zgodna ze standardem 802.3ad. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. Obsługa routingu statycznego. Port-mirroring. Uwierzytelnianie 802.1x na poziomie portu. Uwierzytelnianie 802.1x w oparciu o adres MAC. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. Obsługa protokołu sFlow.
6.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none"> Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: <ul style="list-style-type: none"> Centralne zarządzanie konfiguracją urządzenia Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania

		<ul style="list-style-type: none"> • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. <ol style="list-style-type: none"> 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
--	--	---

7.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> • System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
8.	Gwarancja oraz wsparcie	<p>System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania do 30.06.2026 roku oraz wsparcie techniczne w trybie 24x7.</p> <p>Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:</p> <ul style="list-style-type: none"> • Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.
9.	Opisy do wymagań ogólnych	<p>1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć</p>

		<p>dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.</p>
--	--	--

3. Switch 24 portowy-2 szt.

L.p.		
1.	Parametry fizyczne platformy	<ul style="list-style-type: none"> Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Maksymalny pobór mocy: 30 W. Minimalny zakres temperatury pracy: 0-40°C.

2.	Interfejsy sieciowe - wymagania minimalne	<p>1. Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:</p> <p>a) 24 porty GE RJ-45. e) 4 porty 10 GE SFP+.</p>
3.	Zarządzanie	<ul style="list-style-type: none"> • Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. • Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
4.	Parametry wydajnościowe	<ul style="list-style-type: none"> • Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-

		<p>speed na wszystkich portach) oraz min. 190 Mpps.</p> <ul style="list-style-type: none"> • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
5.	Wymagane funkcje	<ul style="list-style-type: none"> • Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
6.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none"> 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

		<ul style="list-style-type: none"> • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. <ol style="list-style-type: none"> 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie
--	--	---

		wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
7.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> • System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
8.	Gwarancja oraz wsparcie	<p>System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania do 30.06.2026 roku oraz wsparcie techniczne w trybie 24x7.</p> <ol style="list-style-type: none"> 1. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty: <ul style="list-style-type: none"> • Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

		<ul style="list-style-type: none"> • Certyfikat ISO 9001 podmiotu serwisującego.
9.	Opisy do wymagań ogólnych	<ol style="list-style-type: none"> 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

4. Centralny systemu logowania i raportowania

Lp.		
1	Wymagania Ogólne	W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2	Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> 1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45. 2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB. 3. System musi być wyposażony w zasilanie AC.
3	Parametry wydajnościowe	
W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:		
4	Logowanie	<ol style="list-style-type: none"> 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: <ol style="list-style-type: none"> a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników.

		<p>c. Listę najczęściej wykorzystywanych aplikacji.</p> <p>d. Listę najczęściej odwiedzanych stron www.</p> <p>e. Listę krajów , do których nawiązywane są połączenia.</p> <p>f. Listę najczęściej wykorzystywanych polityk Firewall.</p> <p>g. Informacje o realizowanych połączeniach IPSec.</p> <p>4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.</p> <p>5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.</p> <p>6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.</p>
5.	Raportowanie	<p>W zakresie raportowania system musi zapewniać:</p> <ol style="list-style-type: none"> 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

6.	Korelacja logów	<p>W zakresie korelacji zdarzeń system musi zapewniać:</p> <ol style="list-style-type: none"> 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: <ul style="list-style-type: none"> • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.
7.	Zarządzanie	<ol style="list-style-type: none"> 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. <ol style="list-style-type: none"> a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
8.	Gwarancja oraz wsparcie	<p>Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy polegającym na naprawie lub wymianie urządzenia w przypadku jego</p>

		<p>wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania do 30.06.2026 roku oraz wsparcie techniczne w trybie 24x7.</p> <ul style="list-style-type: none"> • Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty: • Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.
9.	Opisy do wymagań ogólnych	<p>1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z</p>

		<p>2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.</p>
--	--	---

5.Accespoint-1 szt.

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

- Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - Temperatura -20 – 45°C,
 - Wilgotność 5–90%.
- Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
- Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
 - 2.4 GHz 802.11b/g/n,
 - 5 GHz 802.11a/n/ac.
- Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
- Urządzenie musi być wyposażone w moduł BLE.
- Urządzenie musi być wyposażone w jeden interfejs 10/100/1000 Base-TX.
- Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
- Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - Tunnel,
 - Bridge,
 - Mesh.

9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - a. MIMO – 2x2,
 - b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 400 Mbps;
 - ii. 867 Mbps;
 - c. Wymagana moc nadawania:
 - i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - ii. min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - d. Wsparcie dla 802.11n 20/40Mhz HT,
 - e. Wsparcie dla kanałów 80MHz,
 - f. Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
 - g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
 - h. Maksymalna deklarowana liczba klientów per moduł radiowy:
 - i. 512;
 - ii. 512;
12. Funkcje dodatkowe:
 - a. 802.11ac MU-MIMO Wave 2
 - b. Transmit Beam Forming (TxBF)
 - c. Low-Density Parity Check (LDPC) Encoding
 - d. Maximum Likelihood Demodulation (MLD)
 - e. Maximum Ratio Combining (MRC)
 - f. A-MPDU and A-MSDU Packet Aggregation
13. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania do 30.06.2026 roku oraz wsparcie techniczne w trybie 24x7.

6. Odnowienie licencji UTM Fortigate 40F dla jednostek podległych – 2szt.

FortiCare Premium i FortiGuard Unified Threat Protection (UTP) do 30.06.2026 roku
FGT40FTK23017250, FGT40FTK23014306

7. Akcesoria dodatkowe

- Wkłady optyczne SFP+ SM 10G - 14 szt. (kompatybilne z oferowanym sprzętem- dopuszcza się zamienniki)
- Kable DAC (SFP+, 10G) 3m – 10 szt.