ZI.272.23.2025
ZAŁĄCZNIK NR 1

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ):

PRZEDŁUŻENIE LICENCJI SERWISÓW POSIADANYCH 25 SZT. UTM FORTIGATE O 24 MIESIĄCE WRAZ Z MODERNIZACJĄ URZĄDZEŃ.

W ramach realizacji przedmiotu zamówienia Zamawiający wymaga zachowania pełnej kompatybilności z już posiadaną przez Zamawiającego infrastrukturą informatyczną oraz oprogramowaniem i nie może w żadnym stopniu ograniczać jej funkcjonalności. Elementy, których to dotyczy, pracować będą w środowisku opartym o posiadane przez Zamawiającego kontrolery domeny Active Directory i rozwiązania Fortinet w tym FortiManager służący do zarządzania flotą urządzeń.

Zamawiający informuje, że jest obecnie w posiadaniu floty 25 szt. urządzeń UTM FortiGate firmy Fortinet, z czego 22 szt. Fortigate 50E (urządzenia te podlegają modernizacji do poziomu funkcjonalności modelu FortiGate 60F) oraz 3 szt. urządzeń FortiGate 60F.

W ramach zamówienia zostaną zrealizowane, zakupione i dostarczone następujące elementy zamówienia w określonych ilościach, zgodne z poniższymi wymaganiami specyfikacji technicznej oferowanego towaru:

1.	**[22 szt.]**	**Przedłużenie niezbędnych serwisów Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) na 24 miesiące wraz z modernizacją posiadanych 22 szt. urządzeń UTM FortiGate 50E do poziomu funkcjonalności UTM FortiGate 60F**
Nazwa elementu, parametru lub cechy		Wymagania
Model i numer seryjny urządzeń do przedłużenia licencji serwisów i modernizacji		W przypadku konieczności przekazania numerów seryjnych posiadanych urządzeń FortiGate 50E do wyceny i złożenia oferty prosimy o przesłanie stosownej wiadomości do Zamawiającego poprzez Platformę Zakupową na stronie postępowania.
Wymagania podstawowe		1) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 2) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. 3) System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. 4) Rozwiązanie musi pozwalać na aktualizację oprogramowania urządzeń do wersji 7.4 i nowszych. 5) Dostarczone rozwiązanie musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 6) Zamawiający dopuszcza w ramach modernizacji możliwość dostarczenia nowych urządzeń FortiGate 60F.

Redundancja, monitoring i wykrywanie awarii	1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3) Monitoring stanu realizowanych połączeń VPN. 4) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1) System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. 2) System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4) System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1) W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps. 4) Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. 5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,4 Gbps. 6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2) Kontrola Aplikacji. 3) Poufność transmisji danych - połączenia szyfrowane IPSec VPN 4) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5) Ochrona przed atakami - Intrusion Prevention System. 6) Kontrola stron WWW. 7) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8) Zarządzanie pasmem (QoS, Traffic shaping). 9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

Polityki, Firewall	1) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
Połączenia VPN	1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • 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. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site.
Routing i obsługa łączy WAN	1) W zakresie routingu rozwiązanie zapewnia obsługę: • Routingu statycznego. • Policy Based Routingu • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

	3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4) System 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 upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
Kontrola aplikacji	1) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2) Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • 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) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6) Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4) Musi istnieć możliwość logowania do serwera SYSLOG.
Serwis i licencja	1) W ramach postępowania powinny zostać dostarczone licencje Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. 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 na okres gwarancji producenta trwającej przynajmniej 24 miesiące.
Gwarancja oraz wsparcie	1) System musi być objęty gwarancją producenta przez okres 24 miesięcy, polegającą na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tej gwarancji producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

	2) Wykonawca musi zapewnić pierwszą linię wsparcia przez okres 24 miesięcy w języku polskim w trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty należy przekazać do wglądu na wezwanie Zamawiającego.**
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.

Koniec tabeli.

2.	**[3 szt.]**	**Przedłużenie licencji serwisów Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) na 24 miesiące**
Nazwa elementu, parametru lub cechy		Wymagania
Wymagania techniczne		Przedłużenie licencji serwisów na poziomie Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) na 24 miesiące dla 3 sztuk UTM FortiGate 60F.
Model i numer seryjny		W przypadku konieczności przekazania numerów seryjnych posiadanych urządzeń FortiGate 60F do wyceny i złożenia oferty prosimy o przesłanie stosownej wiadomości do Zamawiającego poprzez Platformę Zakupową na stronie postępowania.

Koniec tabeli.

Warunki wymagane do spełnienia przez Wykonawcę zamówienia:

1. Cena dotyczy przedmiotu opisanego w Szczegółowym Opisie Przedmiotu Zamówienia (OPZ).
2. Wykonawca dostarczy wszystkie elementy przedmiotu zamówienia do Urzędu Miejskiego w Wołominie.
3. Wykonawca zobowiązany jest do:
- przedłużenia licencji serwisów zgodnie z OPZ;
- dostawy elementów wraz niezbędnymi licencjami, oprogramowaniem oraz z pełnym zestawem okablowania i akcesoriów dołączanych przez producenta oraz dodawanych przez Wykonawcę, niezbędnym do w pełni funkcjonalnej pracy;
- dostawy w przypadku elementów powtarzalnych, identycznych modeli w identycznej konfiguracji;
- dostawy sprzętu o nienaruszonych plombach gwarancyjnych podzespołów bazowych;
- pokrycia wszelkich kosztów załadunku, transportu, rozładunku oraz dostarczenia do wskazanego pomieszczenia zlokalizowanego w siedzibie Zamawiającego.
4. Wykonawca oświadcza, że oferowany towar jest nowy, nieużywany, nieuszkodzony, nieobciążony prawami osób trzecich oraz spełnia normy bezpieczeństwa. Towar, będący przedmiotem umowy, nie jest również refabrykowany, recertyfikowany, poleasingowy, a każdy oferowany element danej pozycji jest jednakowego producenta, modelu i specyfikacji.
6. Wykonawca oświadcza, że oferowany towar pochodzi z oficjalnej, polskiej dystrybucji.

7. Wykonawca potwierdza, że oferowany towar jest zgodny ze wskazanymi w OPZ obowiązującymi Polskimi Normami i Standardami, posiada deklarację zgodności CE oraz spełnia kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii europejskiej o eliminacji substancji niebezpiecznych.
8. Wykonawca oświadcza, że po trzech nieskutecznych naprawach (lub w przypadku braku możliwości naprawy) dokona wymiany towaru na nowy egzemplarz wolny od wad.
9. W przypadku jakichkolwiek wątpliwości, umożliwienia Zamawiającemu wykonania przed podpisaniem protokołu odbioru (w terminie nie dłuższym niż 3 dni od dostawy), testów zgodności dostarczanego przez Wykonawcę towaru z oprogramowaniem użytkowanym przez Zamawiającego oraz wymiany towaru w przypadku, gdy nie przejdzie on powyższych testów.

Zamawiający informuje, że:
1. Może żądać od Wykonawcy przedstawienia dodatkowych dokumentów potwierdzających spełnienie wymagań w Szczegółowym Opisie Przedmiotu Zamówienia dla oferowanego sprzętu.
2. Warunkiem złożenia oferty jest zapoznanie się z wymaganiami postępowania wraz z załącznikami i ich akceptacja.