Załącznik Nr 1b do SWZ

Szczegółowy opis przedmiotu zamówienia dla części II

Zakup oraz dostawa urządzeń sieciowych UTM wraz z oprogramowaniem

1. Urządzenie sieciowe typu UTM z zintegrowanym system bezpieczeństwa klasy UTM/NGFW wraz z subskrypcją zabezpieczeń i gwarancją – 2 sztuki

Specyfikacje minimalnych wymagań:

ARCHITEKTURA SYSTEMU
1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej. 2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19’’ 2. Podwójne, redundantne, zintegrowane zasilanie. 3. Obsługa nielimitowanej ilości hostów w sieci chronionej. 4. Minimalna liczba i typ interfejsów fizycznych: •System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 2,5 Gbps •System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 1GbE (SFP) •System realizujący funkcję Firewall musi umożliwiać rozbudowę dostępnych interfejsów •Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. 5. Minimalna liczba nowych połączeń na sekundę: 30 000. 6. Minimalna liczba jednoczesnych połączeń: 600 000. 7. Minimalna przepustowość Firewall: 10 Gbps.

8. Minimalna przepustowość IPS: 5 Gbps. 9. Minimalna przepustowość Threat Protection: 1,3 Gbps. 10. Minimalna przepustowość IPSec VPN: 2,5 Gbps. 11. Minimalna liczba tuneli SSL VPN: 150. 12. Minimalna liczba tuneli IPSEC VPN: 1000. 13. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania.

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	1. Rozwiązanie musi być zarządzane przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego. 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP. 10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 11. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).

Zapora sieciowa, konfiguracja sieciowa oraz routing	1. Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia. 3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking). 7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 8. Rozwiązanie musi zapewniać obsługę routingu statycznego. 9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). 10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. 11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. 12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. 13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. 15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe. 16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

	21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
Podstawowe kształtowanie pasma oraz limity ilości danych	1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia. 2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP. 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory. 4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android 3. Rozwiązanie musi umożliwiać zmianę hasła.
Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK). 2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	1. Dodatkowy modułochrony klasy IPS z bazą minimum 1000 sygnatur. 2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.

	4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur. 5. System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym. 4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 5. System musi filtrować pliki na podstawie MIME. 6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 7. Rozwiązanie musi zawierać przynajmniej 78 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
Ochrona i kontrola aplikacji	1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	1. Rozwiązanie ma posiadać komercyjny silnik antywirusowy dostarczany od europejskiego dostawcy.

	2. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy. 3. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 4. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 5. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 6. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 7. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 8. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 9. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	Rozwiązaniem musi posiadać dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności: 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe 2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows.
LOGOWANIE I RAPORTOWANIE	
	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).

	5. Rozwiązanie musi generować raporty w HTML i CSV. 6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 7. System musi zapewniać podgląd wykorzystania łącza internetowego. 8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP 9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
POZOSTAŁE	
Certyfikaty	Urządzenie musi posiadać: – certyfikat Common Criteria (zgodny z PN-EN ISO/IEC 15408) na poziomie EAL4 lub wyższym dla odpowiedniego profilu ochrony, lub równoważny dokument potwierdzający spełnienie wymagań bezpieczeństwa funkcjonalnego i odporności na zagrożenia, - certyfikat ICSA Labs dla funkcji VPN IPsec lub równoważny certyfikat niezależnej organizacji certyfikującej zgodność funkcji VPN z międzynarodowymi standardami bezpieczeństwa, lub znajdować się na liście produktów dopuszczonych do ochrony informacji niejawnych UE lub równoważnej liście uznawanej przez instytucje unijne w zakresie kryptografii. **Dokumenty potwierdzające powyższe należy załączyć do oferty.**
W ramach zamówienia Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający: • bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania licencji, • dostęp do dokumentacji sprzętu i oprogramowania, • dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej, • dostęp do pomocy technicznej producenta. Zamawiający w momencie odbioru otrzyma: • licencje obejmujące wszystkie wymagane moduły na okres **do 25.03.2026 r.** • możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.	

2. Warunki gwarancji i serwisu

1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 24 miesięcy dla każdego z urządzeń. **UWAGA:** wydłużenie okresu gwarancji stanowi Kryterium II oceny oferty.
2. Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań.
3. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący usługę rozszerzonej gwarancji typu NBD (Next Business Day) musi

posiadać aktualny certyfikat systemu zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001 lub dokument równoważny, potwierdzający wdrożenie i stosowanie środków zapewniających bezpieczeństwo informacji w zakresie świadczenia usług serwisowych, wsparcia technicznego i gwarancyjnego. **Dokumenty potwierdzające powyższe należy załączyć do oferty.**

4. Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8:00 – 17:00), e-mail lub www (przez całą dobę).

3. Wymagania ogólne dla dostarczanych rozwiązań

1. Dostarczone oprogramowanie musi być fabrycznie nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych.
2. Dostarczony SPRZĘT, musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2024 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta/dystrybutora). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished".
3. Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta.
4. Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

4. Miejsce dostawy, montażu, serwis posprzedażowy

1. Dostawa oraz konfiguracja nowych urządzeń sieciowych UTM w serwerowniach:
   a) **Urząd Miasta Mława, ul Stary Rynek 19, 06-500 Mława,**
   b) **Centrum Usług Społecznych w Mławie, ul. Lelewela 7, 06 – 500 Mława**.
2. Zamawiający wymaga, aby Wykonawca w ramach dostawy zagwarantował Zamawiającemu:
   a) analizę aktualnej struktury sieci lokalnej oraz obecnie funkcjonujących u Zamawiającego starych UTMów(,które będą wymienione) pod kątem instalacji/konfiguracji nowych rozwiązań klasy UTM.
   b) instalacja/konfiguracja zaoferowanego rozwiązania w infrastrukturze sieciowej Zamawiającego musi być wykonana przynajmniej na równoważnym poziome konfiguracji i funkcjonalności z obecnie działającymi starymi UTMami u Zamawiającego oraz zgodnie z wymaganiami Zamawiającego (dotyczy polityk bezpieczeństwa, dostępów zdalnych, integracji z domeną lokalną. Instalacja musi się odbyć fizycznie w siedzibie Zamawiającego – nie dopuszcza się wykonania prac w trybie zdalnym),
   c) po zakończeniu instalacji – instruktarz z wykonanej konfiguracji na zainstalowanym środowisku UTM,

d) 3 miesięczną dedykowaną opiekę poinstalacyjną realizowaną zdalnie – wymagane jest, aby do opieki wyznaczony był dedykowany inżynier z certyfikatem producenta dostarczonego sprzętu. Wsparcie musi być świadczone w dni robocze w godzinach 8:00 – 16:00.