OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Część I – Dostawa i wdrożenie urządzeń bezpieczeństwa sieciowego klasy UTM/NGFW

I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest dostawa **4 sztuk fabrycznie nowych urządzeń bezpieczeństwa sieciowego klasy UTM / Next-Generation Firewall (NGFW)** wraz ze zintegrowanymi licencjami bezpieczeństwa oraz wsparciem technicznym producenta na okres **36 miesięcy (3 lat)**, a także **świadczenie usługi migracji konfiguracji, wdrożenia i uruchomienia** dostarczonego sprzętu w infrastrukturze Zamawiającego.

2. W ramach realizacji zamówienia Wykonawca zobowiązany jest do odbioru od Zamawiającego dotychczas eksploatowanych urządzeń (wyszczególnionych w Rozdziale IV) oraz uwzględnienia ich wartości/upustu z tytułu ich przekazania w ogólnej cenie oferty. Zamawiający dopuszcza realizację tego obowiązku w szczególności poprzez wykorzystanie programów modernizacji i wymiany sprzętu oferowanych przez producentów (np. typu Trade-Up / Trade-In) lub w ramach analogicznych procedur własnych Wykonawcy, pod warunkiem zapewnienia wymiany sprzętu na fabrycznie nowy oraz bezpiecznego odbioru/utylizacji urządzeń wycofywanych.

II. Kontekst infrastrukturalny i wymogi kompatybilności

1. Zamawiający informuje, że jego obecna infrastruktura sieciowo-bezpieczeństwa oraz systemy zarządzania są w całości oparte o rozwiązania marki **Fortinet (system operacyjny FortiOS)**.

2. Oferowane urządzenia UTM muszą zapewniać pełną, natywną i bezproblemową integrację z posiadanym środowiskiem bez konieczności dokupywania dodatkowych licencji, systemów pośredniczących lub przeprowadzania modyfikacji obecnej architektury sieciowej.

3. Wymagane jest, aby oferowane urządzenia:

    - Współpracowały bezpośrednio z posiadanym przez Zamawiającego systemem centralnego zarządzania i raportowania dedykowanym dla systemu FortiOS.
    - Umożliwiały bezproblemowe przeniesienie obecnej polityki bezpieczeństwa, reguł routingu oraz konfiguracji tuneli VPN bezpośrednio z dotychczasowych urządzeń, przy użyciu standardowych narzędzi migracyjnych dostarczanych przez producenta.
    - Wspierały natywne mechanizmy współdzielenia informacji o zagrożeniach w ramach istniejącego środowiska bezpieczeństwa sieciowego Zamawiającego.

III. Minimalne wymagania techniczne i funkcjonalne urządzeń

Dostarczone urządzenia muszą spełniać co najmniej poniższe parametry wydajnościowe i sprzętowe:

Lp.	Parametr / Funkcjonalność	Minimalne wymagania Zamawiającego
1.	**Architektura sprzętowa**	Urządzenie w obudowie kompaktowej (Desktop) wyposażone w **dedykowany procesor sprzętowy typu ASIC** (Application-Specific Integrated Circuit) lub dedykowany układ SOC (System on a Chip) najnowszej generacji, realizujący sprzętową akcelerację przetwarzania ruchu sieciowego oraz funkcji bezpieczeństwa sieciowego w locie.
2.	**Wbudowana pamięć masowa**	Urządzenie musi posiadać wbudowaną pamięć masową typu **SSD o pojemności minimum 120 GB** z przeznaczeniem na przechowywanie logów systemowych, raportowanie lokalne, kwarantannę oraz buforowanie pakietów.
3.	**Interfejsy sieciowe**	Każde z 4 urządzeń musi posiadać fizycznie wbudowane porty w liczbie nie mniejszej niż: • **2 x porty 10 GE SFP+** (wspierające prędkości 10 Gb/s lub 1 Gb/s dla światłowodów/miedzi); • **2 x porty współdzielone (Shared Media)** 10 GE RJ45 / SFP+; • **8 x portów LAN/WAN 1 GE RJ45**.
4.	**Wydajność Firewall (UDP)**	Minimum **27 Gb/s** dla pakietów UDP (1518/512/64 bajty).
5.	**Wydajność IPS**	Minimum **4.5 Gb/s**.
6.	**Wydajność NGFW**	Minimum **2.5 Gb/s** (przy włączonej kontroli aplikacji i systemie IPS).
7.	**Wydajność Threat Protection**	Minimum **2.2 Gb/s** (przy włączonym IPS, kontroli aplikacji, antywirusie oraz filtrowaniu URL).
8.	**Inspekcja ruchu SSL (SSL Inspection)**	Przepustowość inspekcji SSL na poziomie minimum **2.4 Gb/s**.
9.	**Pojemność systemu**	• Obsługa minimum **1 500 000 współbieżnych sesji TCP**. • Obsługa minimum **5000 polityk bezpieczeństwa** (Firewall Policies).

10.	**Bezpieczeństwo połączeń**	• Przepustowość tuneli IPsec VPN: minimum **25 Gb/s**. • Obsługa połączeń szyfrowanych dla pracowników zdalnych (np. standardy IPSec lub równoważne bezpieczne protokoły tunelowania VPN).
11.	**Wysoka dostępność (HA)**	Architektura urządzenia musi wspierać natywną pracę w klastrze niezawodnościowym w trybach Active-Active oraz Active-Passive.
12.	**Zestaw montażowy do szafy Rack 19"**	• Dla każdego z 4 urządzeń Wykonawca musi dostarczyć dedykowany zestaw montażowy pozwalający na instalację w szafie o rozstawie 19 cali, o wysokości maksymalnie 1U. • Zestaw montażowy musi posiadać **specjalne, dedykowane miejsce (kieszeń, uchwyt lub mocowanie) na umieszczenie i unieruchomienie zewnętrznego zasilacza sieciowego** wewnątrz konstrukcji uchwytu. Rozwiązanie to musi zapobiegać luźnemu zwisaniu zasilacza lub okablowania w szafie rackowej. • Konstrukcja zestawu montażowego musi zapewniać swobodny przepływ powietrza chłodzącego urządzenie oraz zasilacz, a także pełen dostęp do portów sieciowych i diod sygnalizacyjnych na przednim panelu. • W komplecie z każdym zestawem muszą znajdować się wszystkie niezbędne śruby montażowe oraz nakrętki klatkowe (koszyczki M6) do profili rack.

1. Wydajność i architektura sprzętowa

- **Przepustowość zapory sieciowej (Firewall throughput):** min. 25 Gb/s.
- **Przepustowość ochrony przed zagrożeniami (Threat Protection):** min. 2,0 Gb/s.
- **Przepustowość systemu zapobiegania włamaniom (IPS):** min. 4,0 Gb/s.
- **Konstrukcja sprzętowa:** Urządzenie oparte o dedykowaną architekturę sprzętową (dedykowane procesory bezpieczeństwa typu ASIC lub równoważne), zapewniającą sprzętową akcelerację przetwarzania ruchu sieciowego oraz deszyfracji ruchu SSL/TLS.
- **Pamięć wewnętrzna:** Wbudowany dysk twardy typu SSD o pojemności min. 120 GB, przeznaczony na potrzeby lokalnego logowania zdarzeń (logów), generowania raportów oraz buforowania danych (odpowiednik modeli z wbudowaną pamięcią masową).

2. Interfejsy sieciowe i fizyczne

- Min. 8 portów miedzianych LAN/WAN w standardzie 1GE (RJ45).

- Min. 2 porty o prędkości min. 10GE (np. współdzielone porty RJ45/SFP+) dedykowane do połączeń uplink.
- Urządzenie musi posiadać dedykowany port konsolowy oraz port USB.

3. Pakiet licencji bezpieczeństwa i wsparcia (na okres 36 miesięcy dla każdego urządzenia)

Każde z 4 urządzeń musi zostać dostarczone z aktywnym pakietem subskrypcji oraz wsparcia technicznego producenta o parametrach nie gorszych niż pakiet **Unified Threat Protection (UTP)** oraz **FortiCare Premium**, obejmujący:

- **Wsparcie techniczne producenta (24x7x365):** Całodobowy dostęp do wsparcia inżynieryjnego producenta, prawo do pobierania i instalowania poprawek oraz nowych wersji systemu operacyjnego (firmware).
- **GWARANCJA sprzętowa i serwis:** Wymiana uszkodzonego urządzenia realizowana bezpośrednio przez producenta w trybie zaawansowanej wysyłki sprzętu zamiennego (Advanced Hardware Replacement) w następnym dniu roboczym od momentu akceptacji zgłoszenia awarii.
- **System zapobiegania włamaniom (IPS):** Ochrona przed podatnościami sieciowymi, atakami typu exploit oraz anomaliami w ruchu.
- **Ochrona przed złośliwym oprogramowaniem:** Zaawansowany antywirus sieciowy, ochrona przed botnetami oraz dostęp do chmurowego systemu analizy zagrożeń typu Sandbox.
- **Filtrowanie treści:** Kontrola dostępu do stron WWW (Web Filtering) oraz filtrowanie zapytań DNS w oparciu o kategorie i reputację adresów.
- **Kontrola aplikacji (Application Control):** Rozpoznawanie i sterowanie ruchem popularnych aplikacji i protokołów sieciowych, niezależnie od używanych portów.

IV. Warunki realizacji programu wymiany sprzętu (Trade-In / Trade-Up)

1. W ramach rozliczenia niniejszego zamówienia i w celu uzyskania upustów cenowych, Zamawiający przekaże Wykonawcy **4 sztuki** dotychczas eksploatowanych, sprawnych urządzeń bezpieczeństwa o następującej specyfikacji:
    - **Producent/Model:** Fortinet FortiGate 60F
    - **Numery seryjne (S/N):**
        - Urządzenie nr 1: FG-60F FGT60FTK20038516
        - Urządzenie nr 2: FG-60F FGT60FTK2109CXFU
        - Urządzenie nr 3: FG-60F FGT60FTK2109CXMB
        - Urządzenie nr 4: FG-60F FGT60FTK19003788

2. **Ciągłość działania sieci:** Ze względu na konieczność utrzymania ciągłości działania systemów teleinformatycznych Zamawiającego oraz czas potrzebny na migrację konfiguracji, fizyczne przekazanie starych urządzeń nastąpi dopiero **po dostarczeniu, uruchomieniu, migracji i podpisaniu bezwarunkowego protokołu odbioru nowych urządzeń**.
3. Zamawiający zobowiązuje się do demontażu i przygotowania starych urządzeń do odbioru w terminie do **14 dni kalendarzowych** od dnia podpisania protokołu odbioru nowego sprzętu.
4. Koszt oraz pełna organizacja transportu starych urządzeń z siedziby Zamawiającego leży po stronie Wykonawcy.
5. Z chwilą fizycznego odbioru starych urządzeń przez Wykonawcę, przechodzą one na jego własność w celu ich utylizacji lub zwrotu do producenta zgodnie z procedurami programu wymiany.

V. Świadczenie usługi migracji konfiguracji i wdrożenia

Wykonawca w ramach realizacji zamówienia zobowiązany jest do wykonania usługi pełnej migracji i uruchomienia nowych urządzeń w środowisku produkcyjnym Zamawiającego, zgodnie z poniższymi wymaganiami:

1. **Prace przygotowawcze i audyt:**
    - Wykonawca dokona pobrania i analizy aktualnych plików konfiguracyjnych ze wszystkich 4 sztuk eksploatowanych urządzeń FortiGate 60F.
    - Wykonawca przygotuje plan migracji uwzględniający specyfikę architektury sieciowej Zamawiającego, mapowanie interfejsów fizycznych (z uwzględnieniem różnic sprzętowych między modelami klasy 60F a docelowymi urządzeniami o wyższej wydajności) oraz harmonogram przełączeń minimalizujący niedostępność usług sieciowych.
2. **Migracja konfiguracji:**
    - Wykonawca dokona konwersji i przeniesienia pełnej konfiguracji sieciowej i bezpieczeństwa ze starych urządzeń na nowe urządzenia.
    - Proces migracji musi obejmować w szczególności: pełną politykę bezpieczeństwa (reguły Firewall), konfigurację interfejsów i VLAN-ów, tabele routingu, translacje adresów (NAT/VIP), konfiguracje tuneli VPN (IPsec / SSL VPN), profile bezpieczeństwa (IPS, Web Filtering, Antivirus, Application Control) oraz bazy użytkowników i certyfikaty.
    - Konwersja konfiguracji musi zostać wykonana w sposób profesjonalny (np. z wykorzystaniem oficjalnego narzędzia Fortinet FortiConverter lub poprzez

ręczne, szczegółowe dostosowanie skryptów konfiguracyjnych), zapewniając pełną integralność logiczną przenoszonych reguł na nowej wersji systemu operacyjnego (FortiOS).

3. **Uruchomienie i testy powdrożeniowe:**
    - Wykonawca dokona fizycznego podłączenia i uruchomienia nowych urządzeń w lokalizacjach wskazanych przez Zamawiającego. Przełączenie ruchu na nowe urządzenia musi zostać przeprowadzone w oknie serwisowym uzgodnionym z Zamawiającym (np. w godzinach popołudniowych lub nocnych).
    - Po przełączeniu ruchu Wykonawca w obecności przedstawiciela Zamawiającego przeprowadzi testy weryfikacyjne potwierdzające prawidłowość działania sieci, w tym m.in.: poprawność routingu, działanie tuneli VPN, poprawność filtrowania ruchu oraz dostępność kluczowych systemów i usług dla użytkowników.
4. **Asysta powdrożeniowa:**
    - Wykonawca zapewni asystę techniczną inżyniera wdrażającego w trybie zdalnym lub stacjonarnym przez okres **2 dni roboczych** od momentu produkcyjnego uruchomienia każdego z urządzeń, w celu natychmiastowego usunięcia ewentualnych problemów wynikających z migracji.

VI. Warunki dostawy i gwarancji

1. Oferowane urządzenia muszą być fabrycznie nowe, pochodzić z oficjalnego i legalnego kanału dystrybucyjnego producenta na rynek europejski oraz posiadać pełne prawo do rejestracji w portalu wsparcia producenta bezpośrednio na dane Zamawiającego.
2. Okres świadczenia usług wsparcia i subskrypcji bezpieczeństwa (36 miesięcy) musi rozpocząć się nie wcześniej niż w dniu podpisania protokołu odbioru urządzeń przez Zamawiającego.
3. Wykonawca dostarczy dokumenty potwierdzające aktywację licencji i wsparcia na dane Zamawiającego najpóźniej w dniu dostawy sprzętu.

VII. Wymagania dotyczące kanału dystrybucji i legalności sprzętu

1. Oferowane urządzenia muszą pochodzić z oficjalnego i autoryzowanego kanału dystrybucyjnego producenta na rynek Unii Europejskiej.

2. Wszystkie licencje, subskrypcje oraz usługi wsparcia technicznego muszą zostać zarejestrowane przez Wykonawcę bezpośrednio na dane teleadresowe Zamawiającego jako pierwszego, legalnego użytkownika końcowego.

3. Początek biegu okresu 36-miesięcznego wsparcia i subskrypcji dla wszystkich 4 urządzeń musi nastąpić nie wcześniej niż w dniu podpisania końcowego, bezusterkowego protokołu odbioru urządzeń przez Zamawiającego.

4. Zamawiający wymaga, aby oferowane urządzenia nie były objęte jakimkolwiek wcześniejszym programem rejestracji, testowania (tzw. "demo" / "NFR") lub rynkiem wtórnym.

3. Wymagania dotyczące pakietu licencji bezpieczeństwa i wsparcia na okres 36 miesięcy

Dla każdego z 4 dostarczonych urządzeń Wykonawca musi dostarczyć i aktywować na okres **36 miesięcy (3 lat)** następujące, zintegrowane pakiety usług, odpowiadające standardem i funkcjonalnością pakietom producenta:

A. Wsparcie techniczne klasy Premium (odpowiednik: FortiCare Premium)

- **Dostępność:** Usługa wsparcia inżynieryjnego świadczona bezpośrednio przez producenta urządzenia w trybie **24/7/365** przez cały 36-miesięczny okres umowy.
- **Kanały kontaktu:** Możliwość zgłaszania incydentów drogą telefoniczną, poprzez dedykowany portal WWW oraz czat techniczny live.
- **Czas reakcji (SLA):** Maksymalny czas reakcji inżyniera producenta na zgłoszenie o najwyższym priorytecie (całkowita awaria systemu / brak ruchu) wynosi **1 godzinę**.
- **Aktualizacje:** Prawo do bezpłatnego pobierania i instalowania wszystkich poprawek bezpieczeństwa, aktualizacji silników skanujących oraz nowych wydań systemu operacyjnego (firmware) wydanych przez producenta w okresie 3 lat.
- **Gwarancja i wymiana sprzętu (Advanced Hardware Replacement):** W przypadku awarii sprzętowej, której nie uda się rozwiązać zdalnie, producent urządzenia zapewni dostawę sprawnego sprzętu zamiennego w formule **NBD (Next Business Day)** na adres wskazany przez Zamawiającego.

B. Zintegrowane usługi bezpieczeństwa (odpowiednik: FortiGuard Unified Threat Protection - UTP)

Pakiet musi obejmować pełny, zintegrowany zestaw sygnatur i baz wiedzy o zagrożeniach sieciowych, aktualizowany w trybie ciągłym (w czasie rzeczywistym) bezpośrednio z chmury laboratoriów badawczych producenta przez okres **36 miesięcy**:

- **IPS (Intrusion Prevention System):** System zapobiegania włamaniom chroniący przed znanymi i nowo odkrytymi podatnościami aplikacyjnymi, exploitami, atakami sieciowymi oraz atakami typu DoS/DDoS.
- **Advanced Malware Protection (Zaawansowana ochrona przed złośliwym oprogramowaniem):** Ochrona antywirusowa realizowana w locie na poziomie bramy sieciowej, wzbogacona o analizę behawioralną oraz automatyczną integrację z

chmurowym środowiskiem Sandbox do bezpiecznej detekcji i izolacji nieznanych zagrożeń (typu zero-day).

- **Application Control (Kontrola aplikacji):** Moduł pozwalający na identyfikację, monitorowanie oraz granularne blokowanie/ograniczanie ruchu dla ponad 5000 aplikacji, niezależnie od dynamicznie zmienianych przez nie portów i protokołów sieciowych.
- **Web Filtering (Filtrowanie zawartości WWW):** Blokowanie dostępu użytkowników do witryn niebezpiecznych, zainfekowanych, phisingowych oraz niezgodnych z polityką Zamawiającego, w oparciu o globalną bazę reputacyjną adresów URL kategoryzowaną w chmurze w locie.
- **Antispam Service (Ochrona poczty):** Moduł weryfikacji i filtrowania ruchu e-mail na bramie, wykrywający wiadomości spamowe, próby wyłudzenia danych (phishing) oraz sprawdzający reputację serwerów pocztowych w czasie rzeczywistym.

4. Klauzula rozwiązań równoważnych (Wymóg PZP)

1. Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych innych producentów niż system, którego parametry posłużyły do zdefiniowania wymagań w niniejszym OPZ.
2. Za rozwiązanie równoważne uznane zostanie urządzenie, które spełnia lub przewyższa wszystkie wymienione w punkcie 2 oraz 3 parametry sprzętowe, wydajnościowe, licencyjne oraz poziom wsparcia technicznego producenta.
3. Wszystkie deklarowane w ofercie wydajności systemu przy włączonych funkcjach bezpieczeństwa (Firewall, IPS, NGFW, Threat Protection, SSL) must be jednoznacznie wynikać z powszechnie dostępnych dokumentacji technicznych (Data Sheet) producenta oferowanego rozwiązania.
4. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca jest zobowiązany dołączyć do oferty dokument potwierdzający, że oferowany system współpracuje bez kosztowo, w pełni kompatybilnie i bez zakłóceń z obecnie posiadaną infrastrukturą sieciową Zamawiającego zbudowaną na urządzeniach firmy Fortinet.

5. Odbiór zamówienia

1. Urządzenia muszą zostać dostarczone w nienaruszonych, oryginalnych opakowaniach fabrycznych, zawierających komplet kabli zasilających, zasilacze oraz **dedykowane 4 zestawy montażowe do szaf Rack 19"** z miejscem na zasilacz.
2. Potwierdzeniem należytego wykonania zamówienia będzie podpisany przez obie strony bezusterkowy Protokół Odbioru Jakościowo-Ilościowego, wygenerowany po weryfikacji numerów seryjnych, poprawności aktywacji licencji na okres 36 miesięcy na dane Zamawiającego w portalu producenta oraz weryfikacji kompletności elementów montażowych.