Załącznik nr 1 do Zapytania ofertowego

Załącznik nr 1 do Umowy CeZ/…/2023

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Część II**

**Zakup urządzenia typu firewall (NGFW)** **Check Point Quantum 6200**

**wraz z usługą wsparcia na okres 12 miesięcy.**

## **Przedmiot zamówienia obejmuje:**

## Dostawę 1 sztuki fabrycznie nowego urządzenia Check Point Quantum 6200, wraz z licencją SandBlast (SNBT) Security Subscription Package (CPAP-SG6200-SNBT).

## Usługę wsparcia świadczoną przez okres 12 miesięcy od daty podpisania protokołu odbioru.

## Gwarancję oraz rękojmię w rozumieniu kodeksu cywilnego na urządzenia wskazane w pkt 1.1. na okres 12 miesięcy od dnia podpisania Protokołu Odbioru wnioskującego o rozliczenie finansowe.

## Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania wskazane do Załączniku nr 1 do OPZ. W przypadku dostarczania urządzenia równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane urządzenie spełnia wszystkie wymagania i warunki określone w Opisie przedmiotu zamówienia.

## **Termin realizacji:**

## Dostawa nastąpi w terminie do 30 dni kalendarzowych od daty podpisania umowy.

## **Usługa gwarancji:**

## W ramach usługi wymagany jest:

## dostęp do strony pomocy technicznej producenta,

## dostęp do aktualizacji oprogramowania,

## dostęp do nowych wersji oprogramowania oraz poprawek,

## dostęp do nowych sygnatur bezpieczeństwa,

## dostęp do bazy wiedzy producenta.

## Usługa musi być świadczona w języku polskim przez producenta lub oficjalnego partnera producenta w zakresie świadczenia pomocy serwisowej.

## Usługa musi być świadczona przez okres 12 miesięcy.

## W ramach świadczenia usługi, w przypadku wystąpienia awarii Zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego.

**Załącznik nr 1 do OPZ:**

## Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania w szczególności w zakresie:

1. funkcjonalności rozwiązania równoważnego, która nie może być gorsza od funkcjonalności urządzenia typu firewall (NGFW) wymienionego w pkt 1.1 OPZ.
2. rozwiązanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
3. rozwiązanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie i systemy informatyczne,
4. rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność rozwiązania równoważnego z wyspecyfikowanym systemem.
5. rozwiązanie równoważne, musi być rozwiązaniem istniejącym na rynku co najmniej 5 lat, pochodzącym z oficjalnego kanału sprzedaży. Jako potwierdzenie spełnienia wymagania uznane będzie zakwalifikowanie oferowanego rozwiązania firewall (NGFW) w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy Network Firewalls w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert).

## Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego następujące wymagania:

1. Firewall:
   1. Rozwiązanie musi zapewnić inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu,
   2. Rozwiązanie musi pozwalać na kontrolę przynajmniej 150 predefiniowanych serwisów/protokołów,
   3. Rozwiązanie musi posiadać możliwość zaraportowania ilości „trafień” wybranej polityki do aplikacji zarządzającej,
   4. Tworzenie reguł musi pozwalać na ich konfigurację w określonych interwałach czasowych wraz z podaniem daty lub godziny ich wygaśnięcia,
   5. Rozwiązanie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory,
   6. Rozwiązaniu musi posiadać lokalną bazę użytkowników pozwalając na ich autentykację bez potrzeby korzystania z zewnętrznych rozwiązań,
   7. Rozwiązanie musi pozwalać na pracę w klastrze wysokiej dostępności w trybie Transparent/Bridge,
   8. Rozwiązanie musi pozwalać na pracę w klastrze wysokiej dostępności oraz w trybie balansowania ruchu (Active/Active),
   9. Praca w trybie Active/Active musi pozwalać na łączenie ze sobą urządzeń w różnych rejonach geograficznych, zlokalizowanych w różnych podsieciach i posiadających różną adresację IP,
   10. Urządzenia pracujące w klastrze mogą posiadać różne wersje uruchomionego firmware,
   11. Rozwiązanie musi umożliwiać budowanie polityki bezpieczeństwa składającej się z wielu warstw logicznych,
   12. Ruch wpadający w daną regułę może zostać przekierowany do inspekcji za pomocą innej warstwy,
   13. Warstwy polityk bezpieczeństwa mogą być współdzielone pomiędzy wieloma różnymi politykami bezpieczeństwa,
   14. Zmiany konfiguracji danej warstwy współdzielonej zostają zastosowane we wszystkich politykach w których ta warstwa występuje dzięki czemu administrator nie musi edytować każdej z polityk osobno.
2. IPS (Intrusion Prevention System):
   1. Zapewnia skuteczność wykrywania zagrożeń i ataków na poziomie minimum 98% udokumentowany przez niezależne testy opublikowane w okresie ostatnich 18 miesięcy (np. niezależne testy NSS Labs),
   2. Musi posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji musza przechodzić przez system),
   3. Musi posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu),
   4. Musi posiadać możliwość wykrywania i uniemożliwiania szerokiej gamy zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługi VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, ataki na systemy SCADA i elementy automatyki przemysłowej, itp.),
   5. Zapewnia co najmniej poniższe sposoby wykrywania zagrożeń:
      * sygnatury ataków opartych na exploitach,
      * reguły oparte na zagrożeniach,
      * mechanizm wykrywania anomalii w protokołach,
      * możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzenia zawartości pakietu,
      * posiada mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives),
      * zapewnia możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.,
      * Posiada możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,
      * Zapewnia możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,
      * Zapewnia mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł musza być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne,
      * Zapewnia możliwość definiowana wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie być zarządzany tylko przez system centralnego zarządzania za pomocą szyfrowanego połączenia,
      * Zapewnia obsługę reguł Snort,
      * Musi mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6,
      * Posiada mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego,
      * Musi chronić protokoły VoIP.
3. Kontrola aplikacji i URL Filtering:
   1. Rozwiązanie musi posiadać co najmniej 6000 sygnatur aplikacyjnych,
   2. Rozwiązanie musi posiadać dedykowane sygnatury dla protokołów ICS/SCADA w tym min. CIP, DNP3, BACNet, EtherCat, IEC 60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, Modbus, OPC DA & UA, Profinet, S7 (Siemens),
   3. Rozwiązanie musi zapewniać kategoryzację 200 milionów adresów URL,
   4. Rozwiązanie musi oferować konfigurację systemu kontroli aplikacji niezależnie od konfiguracji modułu Firewall,
   5. Rozwiązanie musi umożliwiać filtrowanie dla pojedynczej witryny obsługiwanej przez wiele kategorii,
   6. Rozwiązanie musi posiadać przeszukiwalny interfejs graficzny celem przyspieszenia konfiguracji filtra URL oraz aplikacji,
   7. Po za kategoryzacją stron pod względem treści na niej się znajdujących, kategoryzacja obejmuje także ryzyko związane z korzystanie z tej witryny,
   8. Filtrowanie stron WWW odbywa się z weryfikacją użytkownika oraz daje możliwość wyświetlania komunikatów blokady oraz ostrzeżeń w zależności od polityki bezpieczeństwa,
   9. Rozwiązanie musi umożliwiać zapewnienie pasma dla reguł URL Filteringu,
   10. Rozwiązanie musi umożliwiać ograniczenie pasma dla reguł aplikacyjnych np. dla streamingów wideo,
   11. Rozwiązanie musi umożliwiać tworzenie reguł kontekstowych, pozwalających na określenie konkretnego typu plików, które mogą być przesyłane w ramach komunikacji,
   12. Reguły kontekstowe są niezależne od reguł aplikacyjnych, czy reguł Firewalla,
   13. Reguły kontekstowe oraz reguły aplikacyjne umożliwiają integrację bezpośrednio w regułach Firewalla,
   14. Zagnieżdżenie reguł musi dawać możliwość określenia jaki typ pliku jest przesyłany w ramach komunikacji,
   15. Określenie szerokości pasma dostępnego dla aplikacji odbywa się bez wykorzystania mechanizmu QoS.
4. Uwierzytelnienie użytkowników:
   1. Rozwiązanie musi umożliwiać integrację z zewnętrznymi bazami użytkowników w tym Active Directory/LDAP oraz wspiera autoryzację w oparciu o Radius, Kerberos oraz IF-MAP,
   2. Rozwiązanie musi posiadać możliwość autoryzowania użytkowników przez przeglądarkę internetową,
   3. Rozwiązanie musi wspierać autoryzację przez agenta, instalowanego na stacjach lokalnych,
   4. Rozwiązanie musi wspierać autoryzację użytkowników Active Directory bez konieczności instalowania agenta na kontrolerze domeny,
   5. Rozwiązanie musi wspierać zagnieżdżone grupy LDAP,
   6. Rozwiązanie musi wspierać funkcjonalność propagowania tożsamości użytkownika pomiędzy wieloma bramami,
   7. Rozwiązanie musi wspierać uwierzytelnianie dwuskładnikowe przez obsługę wyzwań/odpowiedzi Radius w Captive Portal i trybie RSA SecureID,
   8. Rozwiązanie musi posiadać lokalną bazę użytkowników,
   9. Rozwiązanie musi posiadać funkcjonalność nadawania użytkownikom ról w systemie,
   10. Rozwiązanie musi umożliwiać identyfikację za pomocą serwerów proxy np. za pomocą nagłówka X-Forward.
5. Antywirus i AntiBot:
   1. Rozwiązanie musi być wyposażone w moduł wykrywający złośliwe oprogramowanie oraz moduł wykrywający komunikację z serwerami C&C (Command and Control),
   2. Obydwa moduły musza być zintegrowane z platformą aplikacyjną i granularnie zarządzane za pomocą tej samej konsoli centralnego zarządzania,
   3. Moduł AntiBot musi wykrywać i blokować podejrzane zachowania w chronionych sieciach,
   4. Wykrywanie aktywności botów musi opierać się na wielowarstwowej analizie obejmującej m.in. reputację adresów IP i URL, reputację DNS, analizę cech charakterystycznych dla botnetów,
   5. Rozwiązanie musi umożliwiać wykrywanie malware typu „Cryptor”i „Ransomware” wraz z wariantami „Cryptolocker, CryptoWall, …” itd. Poprzez statyczną i dynamiczną analizę próbki,
   6. Rozwiązanie musi umożliwiać wykrywanie ataków typu „Waterhole”,
   7. Rozwiązanie musi umożliwiać wykonywanie inspekcji ruchu szyfrowanego SSL,
   8. Rozwiązanie musi pozwalać na inspekcję plików skompresowanych,
   9. Rozwiązanie musi umożliwiać skanowanie linków w mailach,
   10. Rozwiązanie musi umożliwiać skanowanie plików przesyłanych protokołem CIFS.
6. Wykrywanie zaawansowanych zagrożeń (Sandbox):
   1. Rozwiązanie musi być wyposażone w moduł prewencyjny eliminujący z dokumentów elementy aktywne będące potencjalnym nośnikiem złośliwego oprogramowania (np. makra dokumentów pakietu Ms Office, javascript w dokumentach typu PDF),
   2. Moduł prewencyjny musi usuwać aktywną zawartość pozostawiając dla użytkownika wyłącznie treść, która jest w pełni bezpieczna,
   3. Moduł prewencyjny może zostać skonfigurowany tak aby przekazywać użytkownikowi oryginalny format dokumentu (np. dokument MS Word pozbawiony makra), lub konwertować wszystkie dokumenty do formatu PDF,
   4. Moduł prewencyjny musi pozwalać zarówno na konwersję plików pobieranych przez przeglądarkę (http, https) jak również plików przesyłanych jako załącznik pocztowy,
   5. Rozwiązanie prewencyjne musi pozwalać użytkownikowi na pobieranie oryginalnej (nie pozbawionej aktywnej zawartości) wersji dokumentu pod warunkiem, że analiza dokumentu w systemie Sandbox nie wykazała obecności złośliwego oprogramowania,
   6. Rozwiązanie musi pozwalać na wykrywanie zaawansowanych zagrożeń poprzez przesyłanie podejrzanych plików do środowiska Sandbox,
   7. Rozwiązanie musi pozwalać na emulowanie w środowisku Sandbox następujących rozszerzeń:
      * .potx
      * .potm
      * .ppam
      * .ppsx
      * .ppsm
      * .rar
      * .rtf
      * .scr
      * .seven-Z
      * .sldx
      * .sldm
      * .swf
      * .tar
      * .tbz
      * .tbz2
      * .tb2
      * .tgz
      * .vbs
      * .vba
      * .vbe
      * .wsf
      * .wsh
      * .xz
   8. Proces analizy plików w środowisku Sandbox może odbywać się w dwóch trybach?
      * Hold – plik zostaje wstrzymany do momentu, kiedy analiza zostanie zakończona,
      * Background – plik zostaje w całości dostarczony do użytkownika, a w tle wysyłany jest dodatkowo do analizy w systemie Sandbox,
   9. Rozwiązanie musi umożliwiać przesyłanie do analizy w środowisku Sandbox plików przesyłanych za pośrednictwem protokołów: HTTP, HTTPS, SMTP, FTP, SFTP, SCP, POP3.
7. IPSec VPN:
   1. System musi umożliwiać realizację połączeń IPSec VPN w trybie Site-to-Site oraz Client-to-Site,
   2. System musi umożliwiać realizację połączeń IPSec VPN w trybie „policy based” oraz „route based”,
   3. System musi umożliwiać konfigurację wielu połączeń IPSec VPN za pomocą GUI i mechanizmu „Drag and Drop”,
   4. System musi posiadać wbudowany moduł CA, umożliwiający generowanie certyfikatów dla urządzeń biorących udział w połączeniu VPN,
   5. System musi wspierać protokół IKE w wersjach 1 i 2,
   6. System musi wspierać grupy DH: 1, 2, 5, 14, 19, 20,
   7. System musi wspierać szyfrowanie Suite-B-GCM-256 oraz kontrolę integralności AES-XCBC,
   8. System musi umożliwiać uwierzytelnienie użytkowników zdalnych za pomocą hasła oraz certyfikatu,
   9. Razem z systemem musi być dostarczony klient VPN.
8. Zgodność:
   1. System przed zastosowaniem zmian, musi kontrolować spójność polityki Firewall i uniemożliwia jej instalacji w przypadku wykrycia niespójności,
   2. System musi być wyposażony w moduł kontroli konfiguracji pod kątem najlepszych praktyk oraz wymagań niezależnych organizacji, przy czym poszczególne wymagania widoczne mają być dla administratora,
   3. System musi umożliwiać wygenerowanie raportu zgodności względem najlepszych praktyk o wymagań niezależnych organizacji.
9. Przepustowość urządzenia i interfejsy:
   1. Urządzenie musi zapewniać przepustowość modułu Firewall na poziomie 9 Gbps,
   2. Urządzenie musi zapewniać przepustowość modułu IPS na poziomie 4,65 Gbps,
   3. Urządzenie musi zapewniać przepustowość modułu NGFW na poziomie 3,72 Gbps,
   4. Urządzenie musi zapewniać przepustowość modułu Threat Prevention (Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, SandBlast) na poziomie 1,8 Gbps,
   5. Urządzenie musi zapewniać do 67 000 nowych połączeń na sekundę,
   6. Urządzenie musi obsługiwać do 2 000 000 jednoczesnych sesji,
   7. Urządzenie musi zapewniać przepustowość VPN na poziomie 2,57 Gbps,
   8. Urządzenie musi być wyposażone w 10 portów 10 Mbps / 100 Mbps / 1 Gbps Ethernet RJ45,
   9. Urządzenie musi posiadać możliwość rozbudowy o kolejne porty, poprzez zakup dodatkowego modułu, np. 8 portów 10 Mbps / 100 Mbps / 1 Gbps Ethernet RJ45, lub 4 portów 1G Base-F SFP, lub 4 portów 10G Base-F SFP+, 4 portów 10 Mbps / 100 Mbps / 1 Gbps Ethernet RJ45, lub 2 portów 10G Base-SR,
   10. Urządzenie musi posiadać możliwość rozbudowy pamięci RAM i umożliwiać rozbudowę pamięci z 8 GB do 16 GB, lub 8 GB do 32 GB, lub z 16 GB do 32 GB,
   11. Urządzenie musi posiadać możliwość dokupienia licencji na ochronę urządzeń IoT,
   12. Urządzenie musi posiadać możliwość dokupienia licencji na uruchomienie SD-WAN.
10. Wszystkie funkcjonalności muszą pochodzić od producenta. W przypadku gdy jakakolwiek funkcjonalność lub parametr ilościowy wymaga licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 12 miesięcy od daty odbioru sprzętu.
11. Wsparcie serwisowe (techniczne) i gwarancja dla urządzenia firewall (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 12 miesięcy od daty odbioru sprzętu.

## W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane rozwiązanie równoważne.

## Rozwiązanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie rozwiązania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie rozwiązania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.