

Załącznik nr 1 do Umowy nr 2025/INF/..... z dnia

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest realizacja zadania polegającego na wymianie systemu zapór sieciowych w Urzędzie Miejskim w Nysie, w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.) poprzez wymianę urządzeń zabezpieczeń ruchu sieciowego czyli dostawę i wdrożenie dwóch nowych urządzeń typu Next Generation Firewall z licencjami, oraz z serwisem gwarancyjnym.

I. Zobowiązania Wykonawcy.

1. Dostarczenie, wdrożenie, uruchomienie i skonfigurowanie systemu zapór sieciowych, z uwzględnieniem konfiguracji i funkcjonalności systemu zapór sieciowych obecnie używanego przez Zamawiającego oraz z uwzględnieniem najlepszych praktyk producenta.
2. Przeprowadzenie razem z Zamawiającym testów akceptacyjnych wdrożonych urządzeń zgodnie z zaproponowanym przez Wykonawcę scenariuszem testów. Testy akceptacyjne będą wykonywane w środowisku produkcyjnym Zamawiającego.
3. Opracowanie Dokumentacji Powykonawczej.
4. Przeprowadzenie warsztatów/konsultacji z zakresu funkcjonowania i administrowania urządzeń.

II. Wymagania wdrożeniowe.

1. Aktualnie Zamawiający posiada dwa urządzenia zabezpieczeń typu Next Generation Firewall (NGFW), pracujące w konfiguracji HA, w trybie Active/Standby. Realizacja przedmiotu zamówienia obejmuje dostawę i wdrożenie **dwóch** urządzeń typu NGFW wraz z niezbędnymi licencjami/subskrypcjami w ilości niezbędnej dla zapewnienia wymaganej funkcjonalności, fabrycznie nowych, nieużywanych we wcześniejszych projektach, pochodzących z legalnego kanału sprzedaży producentów na rynek europejski, zgodnie z wymaganiami i w ilościach określonych w niniejszym opisie.
2. Wdrożenie obejmować będzie uruchomienie dostarczonych urządzeń w środowisku Zamawiającego wraz z integracją z usługami uruchomionymi u Zamawiającego.
3. Wraz z dostawą sprzętu należy dostarczyć dokument, poświadczający datę produkcji sprzętu. Sprzęt nie może być starszy niż 6 miesięcy, licząc od daty podpisania Umowy.
4. Dla oferowanych przez Wykonawcę urządzeń, w dniu złożenia oferty, nie może być opublikowana i ogłoszona przez producenta tego sprzętu data zakończenia ich wsparcia oraz sprzedaży (End-of-Support Date, End-of- Sale Date).
5. Lista usług/programów z którymi trzeba zintegrować wdrożone urządzenia:
 - a) Syslog,
 - b) Active Directory,
 - c) Radius,
 - d) NTP.
6. Zamawiający nie podaje szczegółów istniejącej konfiguracji i wymaga przeprowadzenia analizy konfiguracji dotychczasowego zabezpieczenia sieci Zamawiającego przez Wykonawcę.
7. Po przeprowadzeniu analizy/audytu i uzgodnieniu z Zamawiającym, Wykonawca opracuje Projekt Techniczno - Wykonawczy (PTW) wraz z Harmonogramem Realizacji Wdrożenia (HRW). Zatwierdzenie PTW i HRW przez Zamawiającego będzie pozwalało na dalszą realizację zadania. Przy opracowaniu PTW, Wykonawca będzie kierował się obecną konfiguracją Zamawiającego oraz dobrymi praktykami producenta urządzenia, aby sieć Zamawiającego była zabezpieczona w efektywny sposób.
8. Wykonawca w uzgodnieniu z Zamawiającym opracuje i dostarczy scenariusz testów Akceptacyjnych urządzeń, który będzie obejmował między innymi:
 - a) poprawność konfiguracji urządzeń z wymaganymi funkcjonalnościami,

b) poprawność działania klastra HA.

9. W ramach wdrożenia winno być uruchomione oprogramowanie klienckie VPN na co najmniej 3 komputerach wskazanych przez Zamawiającego oraz komunikacja VPN w ramach natywnej aplikacji VPN na 3 telefonach/tabletach z systemem operacyjnym Android/iOS.
10. Zamawiający zakłada uruchomienie nowego systemu zapór sieciowych w sieci Zamawiającego w okresie realizacji przedmiotu umowy.
11. Realizacja przedmiotu zamówienia nie może w żaden sposób zakłócić lub uniemożliwić prawidłowego funkcjonowania środowiska informatycznego Zamawiającego.
12. Wszystkie prace winny być wykonane z zachowaniem ciągłości dostępu do usług sieciowych przez użytkowników obecnie wykorzystywanej infrastruktury.
13. Zamawiający zapewni wszystkie niezbędne sprzętowe zasoby informatyczne, potrzebne do wdrożenia urządzeń oraz zapewni wsparcie pracowników Wydziału Informatyki w zakresie konfiguracji systemów leżących po stronie Zamawiającego.
14. Zakres integracji wdrażanych urządzeń z systemami Zamawiającego polegać będzie w szczególności na dostarczeniu przez Wykonawcę wymaganych do prawidłowego działania licencji/oprogramowania oraz informacji o koniecznych zmianach w konfiguracji systemów Zamawiającego w postaci instrukcji, opisu konfiguracji itp. Wykonanie wdrożenia urządzeń nie może wpłynąć na poprawne funkcjonowanie sieci Zamawiającego ani żadnych innych systemów teleinformatycznych Zamawiającego.
15. Miejsce realizacji przedmiotu umowy: Urząd Miejski w Nysie, ul. Kolejowa 15, 48-300 Nysa. Na wniosek Wykonawcy, Zamawiający może wyrazić zgodę w formie elektronicznej (e-mail) lub dokumentowej na wykonanie prac zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Zamawiającego.
16. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Zamawiającego.
17. Wykonawca przeprowadzi instalacje i konfiguracje urządzeń zgodnie z najlepszymi praktykami rekomendowanymi przez producenta oraz przeanalizuje razem z Zamawiającym konfigurację posiadanych urządzeń zabezpieczających komunikację i przeniesie wybrane elementy konfiguracji do nowych urządzeń.
18. Wykonawca przeprowadzi wszelkie prace wdrożeniowe w obecności pracownika (lub pracowników) Zamawiającego **w godzinach pracy urzędu** po wcześniejszym uzgodnieniu terminu oraz bez przerwania pracy systemów posiadanych przez Zamawiającego. Za zgodą Zamawiającego, część prac Wykonawca będzie mógł wykonać po godzinach pracy urzędu po wcześniejszym uzgodnieniu terminu.
19. Prace wdrożeniowe musi wykonać specjalista, który wykonywał wdrożenia i posiada ważny certyfikat/oświadczenie producenta, potwierdzający wiedzę w zakresie administrowania i/lub konfigurowania oferowanych urządzeń. Zamawiający ma prawo żądać jego okazania.

III. System zapór sieciowych (2 urządzenia).

Lp.	Nazwa komponentu (element/cecha)	Opis wymaganych minimalnych parametrów technicznych
1.	Obudowa	Urządzenie musi być przeznaczone do montażu w szafie Rack 19" i jego wysokość nie może przekroczyć 1U. Urządzenie musi być dostarczone z wszystkimi niezbędnymi elementami umożliwiającymi montaż urządzenia w szafie.
2.	Porty	Urządzenie musi posiadać: <ol style="list-style-type: none"> a) co najmniej 12 portów 1-Gigabit Ethernet RJ45, b) co najmniej 6 portów 1 Gigabit Ethernet SFP oraz co najmniej 4 porty 10 Gigabit Ethernet SFP+ obsługujące moduły optyczne SR oraz LR, c) co najmniej 1 port 1-Gigabit Ethernet RJ45 wyłącznie do celów zarządzania, d) co najmniej 1 port konsolowy,

		e) co najmniej 1 port (10GE lub szybszy) i port 1-Gigabit Ethernet RJ45 dla celów połączenia urządzeń w klaster (high availability) lub dwa porty 1-Gigabit Ethernet RJ45. Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.
3.	Pamięć	Urządzenie musi posiadać co najmniej 120 GB pojemności dyskowej na przechowywanie logów i firmware.
4.	Zasilanie	Urządzenie musi posiadać co najmniej dwa redundantne zasilacze. Zamawiający nie dopuszcza stosowania zewnętrznych zasilaczy do spełnienia tego warunku. Zasilacze muszą być wymienne z możliwością podmiiany uszkodzonego zasilacza w trakcie pracy urządzenia.
5.	Wydajność urządzenia	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: <ul style="list-style-type: none"> a) 8 Gbps dla rozpoznawania i kontroli aplikacji - przy transakcjach 64KB, b) 4 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: włączone wszystkie sygnatury IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na dyski urządzenia - przy transakcjach 64KB, c) 4 Gbps dla IPSec VPN - przy transakcjach 64KB, d) 90 000 nowych połączeń na sekundę, e) 900 000 jednoczesnych sesji.
6.	Wirtualizacja	<p>Urządzenie musi obsługiwać nie mniej niż 6 wirtualnych routerów, posiadających odrębne tablice routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu, w pojedynczej wirtualnej instancji firewall. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie niż wskazana w pozostałych wymaganiach dla urządzenia.</p> <p>Urządzenie musi posiadać możliwość licencyjnego ustanowienia co najmniej 6 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji - polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablice routingu oraz realizacji zdalnego dostępu.</p>
7.	Funkcjonalności	<p>Urządzenie musi posiadać możliwość zdefiniowania co najmniej 50 stref bezpieczeństwa.</p> <p>Urządzenie musi posiadać architekturę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (Data Plane).</p> <p>Urządzenie musi posiadać wydzielony moduł do zarządzania, tak aby nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie blokowało funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.</p> <p>Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 9900 reguł polityki bezpieczeństwa oraz 2900 reguł NAT.</p>

		<p>Urządzenie musi działać w następujących trybach pracy:</p> <ul style="list-style-type: none"> a) routera (tzn. w warstwie 3 modelu OSI), b) mostu (tzn. w warstwie 2 modelu OSI), c) w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; musi pracować w trybie przezroczystego łączenia interfejsów w pary), d) w trybie pasywnego nasłuchu (sniffer/tap). <p>Urządzenie musi umożliwiać pracę we wszystkich wymienionych powyżej trybach, jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.</p> <p>Urządzenie musi posiadać separację logiczną zasobów służących do przetwarzania ruchu, od zasobów służących do zarządzania urządzeniem.</p> <p>Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.</p> <p>Urządzenie musi wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Podinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać min. 4000 znaczników VLAN.</p> <p>Urządzenie musi wspierać protokół LACP.</p> <p>Urządzenie musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).</p> <p>Urządzenie musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.</p> <p>Urządzenie musi uwzględniać polityki zabezpieczeń:</p> <ul style="list-style-type: none"> a) adresy IP źródłowe i docelowe, b) protokoły i usługi sieciowe, c) aplikacje, d) kategorie URL, e) użytkowników aplikacji i grupy, f) reakcje zabezpieczeń, g) logowanie zdarzeń (początek i koniec sesji), h) strefa wejściowa i wyjściowa. <p>Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzeń.</p>
--	--	---

	<p>Urządzenie musi wykrywać co najmniej 4000 predefiniowanych aplikacji wspieranych przez producenta (takich jak: DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.</p> <p>Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, .vbe, .hta, .wsf, .torrent, .7z, .rar, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.</p> <p>Urządzenie musi obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.</p> <p>Urządzenie musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.</p> <p>Urządzenie musi posiadać osobny zestaw reguł definiujący politykę translacji adresów NAT rozdzielny od polityk innych typów.</p> <p>Urządzenie musi posiadać osobny zestaw reguł definiujący politykę kształtowania ruchu (QoS) rozdzielny od polityk innych typów.</p> <p>Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).</p> <p>Dla fazy 1 i 2 tunelu site-to-site urządzenie musi posiadać wsparcie dla algorytmów szyfrowania minimum AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.</p> <p>Urządzenie musi posiadać osobny zestaw reguł definiujący politykę deszyfracji rozdzielny od polityk innych typów.</p> <p>Urządzenie musi posiadać osobny zestaw reguł definiujący politykę uwierzytelniania rozdzielny od polityk innych typów.</p> <p>W urządzeniu musi być odnotowywane wykonywanie operacji translacji adresów NAT w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.</p> <p>Urządzenie musi pozwalać na selektywne wysyłanie logów na zasoby zewnętrzne w zależności od ich rodzaju.</p> <p>Urządzenie musi zapewniać możliwość odszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.3.</p> <p>Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.</p> <p>Urządzenie musi posiadać możliwość odnotowywania wykonywania operacji odszyfrowania ruchu w logach urządzenia w dedykowanej do tego celu sekcji. Logi muszą zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.</p>
--	--

		<p>Urządzenie musi umożliwiać wykorzystanie mechanizmów filtrowania URL przy wykonywaniu operacji deszyfrowania ruchu.</p> <p>Urządzenie musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.</p> <p>Urządzenie musi posiadać dla deszyfrowania ruchu TLS 1.3 wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256.</p> <p>Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.</p> <p>Urządzenie musi wspierać zarządzanie pasmem (QoS) i ustawienia dla aplikacji priorytetu oraz pasma.</p> <p>Urządzenie musi zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tunelowania SSH.</p> <p>Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywana na dostarczonych urządzeniach, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p> <p>Urządzenie musi posiadać bezpośrednio w GUI możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.</p> <p>Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na dostarczonych urządzeniach.</p> <p>Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół (co najmniej: http, http2, smtp, imap, pop3, ftp, smb). Baza sygnatur antywirusa musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co urządzenie.</p> <p>Urządzenie musi posiadać funkcję antyspyware. Baza sygnatur musi być przechowywana na dostarczonych urządzeniach, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co urządzenie.</p> <p>Urządzenie musi posiadać funkcję filtrowania URL.</p> <p>Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.</p> <p>Urządzenie musi posiadać funkcję filtrowania URL, aby zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.</p> <p>Urządzenie musi posiadać oddzielne kategorie URL dla zagrożeń typu malware, phishing, C&C, ransomware oraz ostatnio zarejestrowane domeny.</p> <p>Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.</p>
--	--	--

		<p>Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox” plików różnych typów (co najmniej: Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, BAT, HTA) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować urządzenie sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze docelowym po ataku. Interwał aktualizacyjny to maksymalnie 2 godziny.</p> <p>Urządzenie musi mieć możliwość konfiguracji, jakiego rodzaju typy plików z listy wspieranych przez funkcję sandbox zostaną wysłane do skanowania przez zewnętrzne systemy realizujące funkcję sandbox.</p> <p>Urządzenie musi wykrywać i blokować zagrożenia DNS w ruchu przechodzącym przez dostarczone urządzenia bez potrzeby rekonfiguracji serwera DNS.</p> <p>Urządzenie musi realizować podstawową ochronę DNS w zakresie:</p> <ul style="list-style-type: none"> a) wykrywania zapytań do domen złośliwych (baza domen musi pochodzić od producenta urządzenia), b) możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing). <p>Urządzenie musi obsługiwać funkcję DNS proxy.</p> <p>Urządzenie musi obsługiwać podstawową funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana z wykorzystaniem SSL oraz IPSec.</p> <p>Urządzenie musi realizować zaawansowaną ochronę DNS w zakresie:</p> <ul style="list-style-type: none"> a) wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA), b) wykrywania domen dynamicznych Dynamic DNS, c) wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych. <p>Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.</p> <p>Urządzenie musi posiadać funkcjonalność pozwalającą na wysyłanie ruchu do narzędzi firm trzecich w celu dodatkowej analizy i detekcji zagrożeń.</p> <p>Urządzenie musi pracować jako para urządzeń wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.</p> <p>Jeżeli w oferowanych urządzeniach, którekolwiek licencje/subskrypcje są czasowe, ograniczające w jakikolwiek sposób funkcjonalności, Zamawiający wymaga dostarczenia licencji/subskrypcji na okres 3 lat od daty podpisania protokołu zdawczo-odbiorczego.</p>
8.	Zarządzanie	<p>Urządzenie musi być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji (lub pobieranie) dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.</p> <p>Urządzenie musi być wyposażone w interfejs API (REST, JSON, XML) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania</p>

	<p>lub linii poleceń (CLI). Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem. Jeżeli dostęp do API urządzenia, jego dokumentacji, zadawania pytań do pomocy, wymaga licencji lub subskrypcji - należy dostarczyć odpowiednie.</p> <p>Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:</p> <ul style="list-style-type: none"> a) bazy lokalnej, b) serwera Radius, c) serwera TACACS+, d) serwera AD/LDAP, e) dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH, a dla dostępu GUI za pomocą certyfikatów kryptograficznych. <p>Urządzenie musi posiadać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:</p> <ul style="list-style-type: none"> a) LDAP, b) Microsoft Active Directory, c) Microsoft Exchange, d) Syslog, e) RADIUS, f) TACACS+. <p>Dostęp i zarządzanie z sieci musi być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).</p> <p>Urządzenie musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.</p> <p>Urządzenie musi posiadać politykę kontroli dostępu, precyzyjnie definiującą prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, mających wspólny źródłowy adres IP, ustalanie tożsamości musi odbywać się również transparentnie.</p> <p>Urządzenie musi pozwalać na lokalne zbieranie (na niemechaniczne zasoby dyskowe w dostarczonych urządzeniach) i analizowanie logów, korelowanie zbieranych informacji oraz budowanie raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu URL, deszyfracji SSL.</p> <p>Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe, jak i umożliwiać tworzenie raportów niestandardowych.</p> <p>Urządzenie musi pozwalać na zapisanie raportów i ich uruchamianie w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.</p>
--	--

		<p>Urządzenie musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach, a proces oznaczania etykiet musi pozwalać na użycie:</p> <ul style="list-style-type: none"> a) reakcji na zdarzenie/log (np. wystąpienie zagrożenia), b) API. <p>Urządzenie musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP oraz etykietach (tagi) dla środowiska VMware ESX i VMware vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.</p>
9.	Oprogramowanie klienckie VPN	<p>Oprogramowanie klienckie w podstawowej funkcjonalności zdalnego dostępu VPN musi wspierać co najmniej poniższe systemy operacyjne:</p> <ul style="list-style-type: none"> a) Windows 10, Windows 11, b) macOS od wersji co najmniej 10.11. <p>Oprogramowanie klienckie Remote Access VPN musi posiadać wsparcie producenta (możliwość zakładania spraw w dziale wsparcia producenta). Jeśli wymaga to dodatkowych licencji/zakupów należy je dostarczyć.</p> <p>Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.</p> <p>Jeżeli oprogramowanie klienckie VPN jest dodatkowo licencjonowane przez producenta oraz wymaga odrębnego kontraktu serwisowego/supportowego, to wówczas należy to przewidzieć i dostarczyć odpowiednie licencje.</p> <p>Oprogramowanie klienckie VPN dla minimum 300 użytkowników.</p>
10.	Gwarancja/ Wsparcie producenta	<p>Trzyletnia gwarancja/wsparcie producenta urządzeń z gwarantowanym czasem reakcji serwisu lub wysyłki części, najpóźniej w następnym dniu roboczym 9x5 (tzw. Next business day). Naprawa realizowana przez producenta urządzeń lub autoryzowany przez producenta serwis w miejscu eksploatacji.</p> <p>Możliwość aktualizacji i pobrania sterowników do oferowanego modelu urządzeń w najnowszych certyfikowanych wersjach, bezpośrednio z sieci Internet za pośrednictwem strony www producenta urządzeń.</p> <p>Telefoniczna linia techniczna producenta umożliwiająca zgłoszenie usterki sprzętowej urządzenia w czasie obowiązywania gwarancji/wsparcia producenta po podaniu numeru seryjnego urządzenia.</p>

IV. Wsparcie powdrożeniowe

1. Konsultacje techniczne, przekazujące wiedzę na temat wdrożonego rozwiązania zostaną przeprowadzone po zakończeniu testów z wynikiem pozytywnym w terminie uzgodnionym z Zamawiającym. Konsultacje techniczne mają pomóc administratorom w kompleksowym podejściu do codziennej administracji.
2. Konsultacje przekazujące wiedzę z zakresu wdrożenia, instalacji i konfiguracji dostarczonych urządzeń muszą objąć minimum następujący zakres merytoryczny:
 - a) omówienie budowy i modułów urządzenia,
 - b) omówienie interfejsów, połączeń sieciowych LAN, WAN, DMZ,
 - c) montaż i podłączenie urządzenia w infrastrukturze Zamawiającego,
 - d) autoryzacja i dostęp do konsoli zarządzającej,
 - e) omówienie konsoli zarządzającej,
 - f) instalacja i konfiguracja,

- g) deszyfracja ruchu SSL,
 - h) połączenia VPN,
 - i) zarządzanie urządzeniem - dobre praktyki.
3. Zamawiający wymaga przeprowadzenia konsultacji przez specjalistę, który wykonywał wdrożenia i posiada ważny certyfikat/zaświadczenie wystawione przez producenta dostarczonego urządzenia, potwierdzający wiedzę w zakresie administrowania wdrożonych urządzeń. Zamawiający ma prawo żądać jego okazania.
4. Zamawiający wymaga przeprowadzenia warsztatów/konsultacji w wymiarze minimum **20** godzin w języku polskim. Zamawiający wymaga przeprowadzenia **1 warsztatu w siedzibie Zamawiającego** w wymiarze łącznym **6 godzin**. Pozostałe godziny mogą być zrealizowane w formie konsultacji zdalnych. Terminy konsultacji będą każdorazowo uzgadniane z Zamawiającym.

V. Dokumentacja.

1. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym, spójnym dokumentem, bez względu na jego objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji urządzeń, w szczególności:
- a) opis architektury wdrożonej u Zamawiającego wraz z użytą adresacją,
 - b) wykaz użytych licencji dla systemu zapór sieciowych,
 - c) opis wdrożonych mechanizmów ochronnych sieci (reguły, polityki),
 - d) procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji urządzeń,
 - e) procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
 - f) instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa, procedury postępowania w razie wystąpienia awarii lub błędów systemu zapór sieciowych,
 - g) instrukcje dla użytkowników i administratorów, opisującą instalację oraz konfigurację oprogramowania klienckiego VPN,
 - h) inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia urządzeń, uzgodnione z Zamawiającym.
2. Dokumentacja musi być napisana w języku polskim, dostarczona w formie papierowej 1 egz. Dodatkowo w wersji elektronicznej w formacie edytowalnym (doc/docx) oraz w formacie graficznym (pdf). Procedury i instrukcje producenta mogą być dostarczone w języku angielskim lub polskim.

VI. Odbiór.

1. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy w zakresie uruchomienia, skonfigurowania urządzeń będzie podpisany bez zastrzeżeń Protokół zdawczo-odbiorczy zawierający w szczególności:
- a) Potwierdzenie kompletności dostawy (urządzeń oraz licencji/subskrypcji),
 - b) Potwierdzenie poprawnej konfiguracji urządzeń na podstawie przeprowadzonych Testów Akceptacyjnych,
 - c) Potwierdzenie dostarczenia Dokumentacji Powykonawczej,
 - d) Potwierdzenie realizacji warsztatów/konsultacji.