ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz usługami wsparcia technicznego i gwarancji.

I.1 Kody CPV

32420000-3 Urządzenia sieciowe.
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.

II. Przedmiot zamówienia

(1) Przedmiotem zamówienia jest dostawa urządzeń systemu klasy NGFW (ang. Next Generation Firewall) wraz z usługami wsparcia oraz gwarancją producenta i świadczeniem w ramach prawa opcji godzin eksperckich na rzecz Zamawiającego.

(2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Dzień Roboczy	oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Godziny ekspercie	usługi konsultacji (tzw. ang. *Professional Services*), których przedmiotem będą miedzy innymi zagadnienia wskazane w OPZ, dotyczące obsługi, konfiguracji I eksploatacji Urządzeń, bieżących problemów dotyczących funkcjonowania Urządzeń, ich konfiguracji, wyjaśniania wątpliwości lub rozwiązania zagadnień z tego zakresu przedstawianych przez Zamawiającego, związanych z obsługą Urządzeń, świadczone w miejscu zainstalowania Urządzeń lub zdalnie, na warunkach wskazanych w OPZ, w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.
Hardware Appliance	ang. Hardware Appliance oznacza urzadzenie fizyczne wraz z oprogramowaniem do którego Producent dostarcza wsparcie techniczne.
Roboczogodzina	jedna godzina pracy członka personelu Wykonawcy.
SSL/TLS	*ang.* Secure Socket Layer / Transport Layer Security oznacza

	protokół szyfrowania komunikacji sieciowej. (ze wsparciem co najmniej w wersji TLS 1.2 lub TLS 1.3).
Urządzenia	oznacza przedmiot zamówienia opisany w pkt. III.1 niniejszego dokumentu.
Wsparcie producenta	oznacza oferowane przez producenta Urządzeń aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych urządzeń przez zdefiniowany okres czasu.

(3) Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym i takim odniesieniom towarzyszą wyrazy "lub równoważne".

(4) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

(5) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

(6) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

(7) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

(8) Wykonawca zobowiązany jest posiadać status partnera producenta NGFW i Konsoli Zarządzającej z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym.

(9) Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji.

III. Specyfikacja wymagań

Przedmiotem zamówienie jest dostawa urządzeń klasy NGFW, opisanych w pkt. III.1 oraz przeprowadzenie ich pierwszej instalacji i uruchomienia, w ramach usług opisanych w pkt. III.2. a następnie świadczenie usług opisanych w pkt. III.2 – III.4.

III.1 Dostawa Urządzeń

Przedmiotem zamówienia jest dostawa:

(a) sześciu urządzeń klasy NGFW (ang. Next Generation Firewall), zwanych dalej „**NGFW**”, w tym:

(i) dwóch **NGFW typu 1,**

(ii) dwóch **NGFW typu 2**

(iii) dwóch **NGFW typu 3,**

(b) dwóch konsol zarządzających w/w NGFW, zwanych dalej „**Konsolami Zarządzającymi**”.

zwanych łącznie „**Urządzeniami**”, w terminie *czterech tygodni*[1] od dnia podpisania umowy.

III.1.1 Wymagania ogólne dla Urządzeń:

Lp.	Opis wymagania	Parametry minimalne
1	Parametry montażowe	Urządzenia fizyczne z przedmiotu zamówienia muszą być przystosowane do montażu w szafach RACK 19” i być dostarczone z odpowiednimi elementami montażowymi.
2	Zasilacze	2.1 Urządzenia wchodzące w skład niniejszego przedmiotu zamówienia muszą być wyposażone w minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug (230V). 2.2 Każde z urządzeń fizycznych wchodzące w skład Systemu NGFW musi posiadać takie

[1] Stanowi kryterium oceny ofert

		zasilacze, że w przypadku awarii jednego z nich, drugi zasilacz umożliwi zasilenie w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych.
3	Jednorodność, szyfrowanie i dodatkowe kryteria bezpieczeństwa	3.1 Urządzenia wchodzące w skład Systemu NGFW muszą pochodzić od tego samego producenta oraz nie mogą znajdować się na liście (typu „end-of-life" oraz „end-of-support"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025. *3.2 NGFW powinno posiadać zodność z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub wyższym lub równoważnym[2];* *3.3 Urządzenia (NGFW i Konsola Zarządzajaca) powinny posiadać zgodność z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile for Network Devices v2.1" lub wyższym lub równoważnym[3].* *3.4 NGFW powinno posiadać zgodność z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways"* w wersji 1.0 lub wyższym *lub równoważnym[4].* 3.5 NGFW i Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny*.

*Zamawiający wskazuje następujące warunki równoważności dla normy FIPS 140-2 lub 140-3 i uzna za normę równoważną opisywanej, normę która:

[2] Wymaganie nie jest obligatoryjne i stanowi kryterium oceny ofert, opisane w Rozdziale I SWZ.
[3] Wymaganie nie jest obligatoryjne i stanowi kryterium oceny ofert, opisane w Rozdziale I SWZ.
[4] Wymaganie nie jest obligatoryjne i stanowi kryterium oceny ofert, opisane w Rozdziale I SWZ.

1. Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
2. Została wydane przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,
3. Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
4. Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.

III.1.2 Wymagania dla urządzeń NGFW

4	Rodzaj i Ilość	Sześć fizycznych urządzeń lub zestawów urządzeń NGFW typu Hardware Appliance tego samego producenta.
5	Wydajność	5.1 Dla NGFW – typ 1: Każdy z dwóch NGFW musi mieć wydajność przetwarzania ruchu sieciowego w trybie ochrony FW (ang. FireWall), IPS (ang. Intrusion prevention systems) i kontroli aplikacji – min. 20 Gbps. 5.2 Dla NGFW – typ 2: Każdy z dwóch NGFW musi mieć wydajność przetwarzania ruchu sieciowego (każdy z nich) w trybie ochrony FW (ang. FireWall), IPS (ang. Intrusion prevention systems) i kontroli aplikacji – min. 10 Gbps. 5.3 Dla NGFW – typ 3: Każdy z dwóch NGFW musi mieć wydajność przetwarzania ruchu sieciowego (każdy z nich) w trybie ochrony FW (ang. FireWall), IPS (ang. Intrusion prevention systems) i kontroli aplikacji – nie mniejsza niż 1 Gbps.
6	Interfejsy fizyczne	**Każdy z dwóch NGFW typu 1 (przetwarzający min. 20 Gbps) musi być wyposażona w:** 6.1 Min. 8 interfejsów 10 Gbps SFP+ z kompatybilnymi wkładkami 10GBase-SR (LC) objętymi tą samą gwarancją co NGFW.

		6.1.1 Kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex. 6.2 Min. 1 interfejs 1 Gigabit Ethernet - wydzielony port do zarządzania (out-of-band). **Każdy z dwóch NGFW typu 2 (przetwarzający min. 10 Gbps) musi być wyposażona w:** 6.3 Min. 8 interfejsów 10 Gbps SFP+ z kompatybilnymi wkładkami 10GBase-SR (LC) objętymi tą samą gwarancją co NGFW. 6.3.1 Kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex. 6.4 Min. 8 interfejsów 1 Gbps SFP. 6.4.1 Dwa komplety kompatybilnych wkładek, tzn. 8 sztuk 1000Base-T oraz 8 sztuk 1000Base-SX (LC) objętymi tą samą gwarancją co NGFW. 6.4.2 Kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex. 6.4.3 Kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 20m, 8x 5m, 8x 2m) w standardzie RJ-45 UTP CAT5e. 6.5 Min. 1 interfejs 1 Gigabit Ethernet wydzielony port do zarządzania (out-of-band). **Każdy z dwóch NGFW typu 3 (przetwarzający min. 1 Gbps) musi być wyposażona w:** 6.6 Min. 8 interfejsów 1Gbps SFP. 6.6.1 Dwa komplety kompatybilnych wkładek, tzn. 8 sztuk 1000Base-T oraz 8 sztuk 1000Base-SX (LC) objętymi tą samą gwarancją co NGFW. 6.6.2 Kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x

		5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex. 6.6.3 Kable sieciowe (ang. Patchcord) kompatybilne z w/w wkładkami (8x 10m, 8x 5m, 8x 2m) w standardzie RJ-45 UTP CAT5e. 6.7 Min. 1 interfejs 1 Gigabit Ethernet wydzielony port do zarządzania (out-of-band).
7	Niezawodność	NGFW (w ramach każdej z par urządzeń NGFW) muszą mieć możliwość działania osobno (jako standalone) jak i posiadać możliwość (licencyjną i techniczną) stworzenia klastra lub użycie machanizmu HA.
8	Asymetryczność i agregacja ruchu	8.1 Ruch pomiędzy dwoma ośrodkami przetwarzania danych (dalej DC) może być asymetryczny i NGFW muszą mieć możliwość zachowania stanu sesji – gdzie pierwsze z pary NGFW będzie w DC1, drugie NGFW z pary będzie w DC2). 8.2 NGFW musi obsługiwać IEEE 802.3ad i agregowanie interfejsów fizycznych z wykorzystaniem protokołu Link Aggregation Control Protocol (LACP).
9	Pamięć wewnętrzna na system operacyjny	Każde z urządzeń NGFW typ 1 i 2 muszą być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej (z możliwością samodzielnego niszczenia dysków przez Zamawiającego), a każde z Urządzeń NGFW typ 3 musi być wyposażone co najmniej w jeden dysk z możliwością samodzielnego niszczenia dysków przez Zamawiającego.
10	Routing i protokół IP	10.1 Musi umożliwić obsługę protokołów routingu m.in.: OSPF, RIP/RIPv2 oraz routing statyczny. 10.2 Musi zapewnić ochronę ruchu sieciowego opartego o protokół IP: IPv4 oraz IPv6. 10.3 Musi umożliwić wykonywanie translacji adresów IP (statycznej i dynamicznej). 10.4 NGFW musi obsługiwać protokół Ethernet wraz z obsługą sieci VLAN.
11	Wymagane modele wdrożeń NGFW	NGFW musi umożliwić ochronę ruchu sieciowego w: 11.1 Drugiej warstwie modelu OSI – L2. 11.2 Trzeciej warstwie modelu OSI – L3.

		11.3 Trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych, przez które przechodzi ruch sieciowy).
12	Tryby pracy IPS w NGFW	12.1 Aktywny (IPS). 12.2 Pasywny (IDS).
13	Kontrola aplikacji	13.1 Musi wykrywać aplikacje w ruchu sieciowym, m.in. P2P (np. torrent), web drive (np. google drive), web mail (np. gmail). 13.2 System musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.
14	Filtrowanie ruchu sieciowego	14.1 Musi zapewniać filtrowanie w oparciu o kategorie (co najmniej): Adult, Gambling, Social Networking, video stream oraz w oparciu o kategorie lub aktualizowaną bazę adresów IP (lub URL) związanych z Malware, Phishing, C&C, TOR (lub TOR Exit Node lub TOR Relay Node), Proxy anonimizujące, przy czym producent dostarcza predefiniowany zestaw kategorii i przypisaną do nich bazę adresów IP lub URL. Baza adresów i kategorii musi być cyklicznie aktualizowania przez Producenta (przez okres wsparcia technicznego). 14.2 Musi zapewnić możliwość ręcznego definiowania dodatkowych kategorii bez użycia zewnętrznych narzędzi oraz możliwość przypisywanie do nich adresów URL i domen.
15	Funkcjonalność aktualizacji i ochrony NGFW	15.1 NGFW musi posiadać moduł wykrywania i blokowania ataków oparty o sygnatury. 15.2 Baza sygnatur moduły inspekcji IPS (ang. Intrusion Prevention System) musi być pobierana (ręcznie i automatycznie) z serwerów producenta na Konsolę. 15.3 Możliwość blokowania ruchu sieciowego na podstawie: • adresów IP • reputacji (IP, domen lub URL) • sygnatur IPS • domen

		• URL • geolokalizacji (np. adresy IP pochodzących z konkretnych państw). 15.4 Rozpoznawanie i blokowanie niedozwolonych aplikacji i protokołów sieciowych. 15.5 Musi umożliwiać automatyczne dodawanie z zewnętrznych serwerów listy (tzw. Feed) zawierających złośliwe adresy IP, domeny lub URL. 15.6 Musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 15.7 Ochrona przed atakami typu flood. 15.8 Możliwość ochrony przed exploitami i blokowanie ruchu sieciowego z nim związanego w celu ochrony podatnych aplikacji lub usług. 15.9 Musi posiadać sygnatury wykrywające i blokujące zapytania DNS i ruch sieciowy do domen uznanych za złośliwe. 15.10 Musi posiadać funkcję wykrywania aktywności sieci typu Botnet. 15.11 Wykrywanie zagrożeń tj. ataki na podatne aplikacje i infrastrukturę. 15.12 Musi odczytywać oryginalne adresy IP z pola „X-Forwarded-For” w nagłówku http. 15.13 Musi umożliwiać tworzenie polityk bezpieczeństwa w oparciu o mechanizmy geolokalizacji. Baza geolokalizacji musi być aktualizowana w sposób automatyczny (przez producenta NGFW).
16	Ochrona IPS - możliwe reakcje na wykryte zdarzenia bezpieczeństwa w przetwarzanym ruchu sieciowym	16.1 Monitoring z alertowaniem. 16.2 Blokowanie. 16.3 Bez inspekcji (aby wybrany na podstawie IP ruch nie był przesyłany do silnika inspekcji IPS).
17	VPN	17.1 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN:

		17.1.1 SSL VPN: w sumie (typ 2 i 3) min. 100 równoległych tuneli oraz 17.1.2 min. 100 tuneli IPSEC per Typ 2 i 3 (w sumie min. 200). 17.2 NGFW typ 1 musi posiadać funkcjonalność zestawiania min. 100 tuneli IPSEC. 17.3 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN typu clientless (Ilość wspieranych równoległych tuneli VPN typu clientless w sumie min. 100) albo należy dostarczyć dedykowane dwa urządzenia umożliwiające: 17.3.1 konfigurację HA (ang. High availability) w trybie active/active. 17.3.2 zestawienie w sumie min. 100 tuneli vpn typu clientless 17.3.3 wraz z systemem musi być dostarczona możliwosć zarządzania (on-prem). 17.3.4 każde z tych urządzeń będą posiadały min. 2 porty SFP, 2 porty SFP+ i port w celu zdalnego zarządzania. 17.3.5 każde z tych urządzeń będzie posiadało dwa zasilacze typu hot-plug. 17.4 NGFW musi posiadać mechanizm terminowania w/w (wszystkich) typów VPN ze wsparciem IPv6 i IPv4. 17.5 VPN w NGFW musi wspierać mechanizm pojedynczego logowania SSO (ang. Single Sign-On). 17.6 Autoryzacja kont vpn musi być możliwa z wykorzystaniem co najmniej usługi katalogowej (AD i LDAP).
18	Zarządzanie pasmem (QoS)	18.1 NGFW musi zapewniać zarządzanie pasmem (QoS) sieci. 18.2 Musi zapewnić limitowanie ruchu sieciowego w oparciu o co najmniej następujące parametry: rozpoznany ruch sieciowy aplikacji oraz adresy IP (źródłowy i docelowy).

19	Kontrola ruchu szyfrowanego	19.1 Musi mieć możliwość przesyłania ruchu zaszyfrowanego (co najmniej TLS/SSL) do zewn. deszyfratora. 19.2 Musi mieć możliwość definiowania polityk bezpieczeństwa w kontekście ruchu szyfrowanego. 19.3 Musi posiadać możliwość deszyfracji ruchu (co najmniej TLS/SSL w oparciu o zaimportowanie klucza prywatnego) w celu jego analizy oraz szyfrowania ruchu z powrotem.

III.1.3 Wymagania dla Konsoli Zarządzających

Wymagania dotyczące Konsoli Zarządzającej		
20	Rodzaj	Wymaga się dostarczenia dwóch Konsol Zarządzających (druga w celu zachowania redundancji) typu Hardware Appliance (lub zestawów urządzeń) tego samego producenta.
21	Niezawodność	21.1 Musi być umożliwiony mechanizm (i licencje) zapewniający redundancje w przypadku awarii jednej z dwóch Konsoli Zarządzających. 21.2 Niedostępność Konsoli Zarządzającej nie może powodować problemów z ruchem przetwarzanym przez NGFW. NGFW muszą realizować przetwarzanie ruchu zgodnie z ostatnią zachowaną konfiguracją.
22	Wymagania funkcjonalne	22.1 Musi umożliwić centralne zarządzanie sondami NGFW, logowanie, analizę i raportowanie zdarzeń bezpieczeństwa. 22.2 Musi umożliwiać generowanie raportów (dot. zarejestrowanych zdarzeń bezpieczeństwa) co najmniej w formatach html lub pdf. 22.3 Musi zapewniać możliwość ręcznego tworzenia sygnatur bezpośrednio na Konsoli.. 22.4 Musi pozwalać na automatyczne usuwanie logów przetrzymywanych na urządzeniu po upływie określonego czasu lub ilości.

		22.5 Musi umożliwić zarzadzanie co najmniej 10-cioma urządzeniami typu NGFW (jeśli istnieje ograniczenie na ilość podłączanych NGFW do Konsoli zarządzającej). 22.6 Zarządzanie urządzeniami systemu musi odbywać się za pomocą graficznej konsoli Web GUI oraz linii poleceń (CLI). Interfejs systemu musi być w języku polskim lub angielskim. 22.7 Musi pozwalać na zdefiniowanie min. 20 administratorów o różnych uprawnieniach. 22.8 Musi być możliwe uwierzytelnienie i autoryzacja użytkowników za pośrednictwem protokołów RADIUS i LDAP. 22.9 Musi umożliwiać budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji NGFW. 22.10 Musi umożliwiać logowanie aktywności administratorów/ użytkowników, zmian w konfiguracji w NGFW i konsoli Zarządzającej z możliwością wysyłania tych logów do systemu klasy SIEM. Nie może być żadnych limitów licencyjnych z tym związanych prócz limitów wydajnościowych. 22.11 Musi umożliwiać zbieranie logów dotyczących połączeń (przechodzących przez NGFW) i przesyłanie tych danych do systemu klasy SIEM wraz z informacją pochodzącej z pola X-Forwarded-For (nie może być żadnych limitów licencyjnych z tym związanych prócz limitów wydajnościowych). 22.12 Musi umożliwiać zbieranie zdarzeń bezpieczeństwa z NGFW wraz z informacją pochodzącej z pola X-Forwarded-For i przesyłanie tych danych do systemu klasy SIEM (nie może być żadnych limitów licencyjnych z tym związanych prócz limitów wydajnościowych). 22.13 Musi umożliwiać zbieranie informacji nt. stanu Urządzeń (monitorowanie wydajności

		i zużycia zasobów) oraz umożliwić ich wysyłanie do zew. systemów.
23	Pojemność dyskowa	23.1 Musi zapewniać przestrzeń dyskową na dane o pojemności nie mniejszej niż 1,6 TB (z możliwością samodzielnego niszczenia dysków przez Zamawiającego.) 23.2 Ilość zarejestrowanych zdarzeń bezpieczeństwa i logi nie mogą być limitowane, . Jedynym ograniczemiem może być ilość zasobów dyskowych Konsoli. 23.3 Musi być możliwość uruchomienia automatycznej rotacji logów np. w przypadku przekroczenia max. przestrzeni dyskowej.

III.2 Zasady realizowania Godzin eksperckich w ramach opcji

(1) Zamawiający wymaga zapewnienia przez Wykonawcę Godzin eksperckich świadczonych przez autoryzowany podmiot współpracujący z producentem przedmiotu zamówienia opisanego w pkt 3.1 powyżej (dalej określanego jako „**Producent**"), w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta – w wymiarze łącznie 1024 Roboczogodzin, przez okres od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt 3.1 powyżej, do końca grudnia 2022r.

(2) Osoba/y realizująca usługi w ramach Godzin eksperckich musi być ekspertem w obszarze związanym z technologią NGFW oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

(3) W ramach usług realizowanych jako Godziny eksperckie będzie m.in. na żądanie Zamawiającego:

(a) opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt (1) powyżej oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Godzin eksperckich,

(b) opracowanie i dostarczenie procedury postępowania w razie wystąpienia incydentów bezpieczeństwa,

(c) opracowanie i dostarczenie procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

(d) konsultacje i wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt II powyżej,

(e) wsparcie i konsultacje dot. utrzymania, eksploatowania, tuningu konfiguracji i reguł/polityk bezpieczeństwa oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez urządzenia stanowiące przedmiot zamówienia, o którym mowa w pkt II powyżej,

(f) montaż urządzeń w serwerowni Zamawiającego,

(4) Osoby realizujące prace w serwerowni Zamawiającego będą zobowiązane na żądanie Zamawiającego, do dostarczenia aktualnego zaświadczenia o niekaralności lub poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli „POUFNE", na min. 7 dni przed rozpoczęciem prac.

(5) Zamawiający wymaga zapewnienia realizacji Godzin eksperckich, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej z Wykonawcą Umowie, wskazujących przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług nie później niż w terminie 3 dni roboczych od dnia przekazania Wykonawcy zlecenia.

(6) Świadczenie usług w ramach Godzin eksperckich uzależnione jest od wcześniejszego zlecenia ich zakresu przez Zamawiającego, poprzez złożenie oświadczenia o skorzystaniu z prawa opcji. Skorzystanie z prawa opcji jest uprawnieniem Zamawiającego, z zastrzeżeniem, że korzystając z prawa opcji, nie jest zobowiązany do zakupienia żadnej ilości Godzin eksperckich, a całość tego świadczenia objęta jest prawem opcji, które nie musi być wykonane przez Zamawiającego. Nieskorzystanie przez Zamawiającego z prawa opcji nie rodzi po stronie Wykonawcy jakichkolwiek roszczeń w stosunku do Zamawiającego.

III.3 Zasady świadczenia usług gwarancji

(1) Wykonawca zobowiązany jest zapewnić Zamawiającemu gwarancję dla przedmiotu zamówienia opisanego w pkt II powyżej, udzieloną przez Producenta tych urządzeń (dalej określanego jako „**Producent**") lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta, obejmującą okres 36 miesięcy, od dnia odbioru sprzętu opisanego w pkt II.

(2) Wykonawca, zobowiązany będzie zapewnić wykonywanie zobowiązań z tytułu Gwarancji, zgodnie z następującymi zasadami:

(a) Zamawiający będzie uprawniony do dokonywania zgłoszeń awarii w trybie 24/7/365, za pośrednictwem telefonu lub dedykowanej aplikacji lub adresu poczty elektronicznej, wskazanych przez Wykonawcę;

(b) Serwis gwarancyjny realizowany będzie w miejscu wskazanym przez Zamawiającego na terenie m.st. Warszawy.

(c) Zgłoszone awarie będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.

(3) W przypadku w którym usunięcie awarii będzie wymagać odinstalowania urządzenia, które uległo awarii:

(a) Naprawa będzie mogła być wykonana wyłącznie w lokalizacji instalacji urządzenia, bez wydawania go poza tą lokalizację;

(b) Wydanie urządzenia poza miejsce jego instalacji, w celu dokonania naprawy, będzie mogło nastąpić dopiero, po trwałym usunięciu danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego.

(4) W przypadku nie przywrócenia pełnej funkcjonalności urządzenia w terminie określonym w pkt (6) powyżej Wykonawca zobowiązuje się zapewnić urządzenie zastępcze na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie oraz zapewniających nie gorszy poziom bezpieczeństwa. W przypadku zwrotu urządzenia zastępczego, Gwarant zapewni trwałe usunięcie danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego. W takim przypadku termin usunięcia awarii przez Gwaranta wynosi 30 dni kalendarzowych od chwili zgłoszenia awarii.

Gwarant zapewni wsparcie techniczne w stosunku do urządzenia zastępczego do czasu naprawienia Urządzenia które uległo awarii.

(5) Gwarant jest zobowiązany do wymiany urządzenia na nowe na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie w przypadku w którym usunięcie awarii o której mowa w pkt. 4 powyżej jest niemożliwe. W takim przypadku Gwarant zapewni wsparcie techniczne w stosunku do nowego urządzenia.

(6) Wykonywania zobowiązań gwarancyjnych, wymagające fizycznego dostępu do lokalizacji instalacji urządzenia, wymagać będzie spełnienia przez osoby wykonujące te czynności w imieniu Gwaranta następujących wymogów:

(a) przedłożenia aktualnego zaświadczenia o niekaralności lub poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli „POUFNE”.

III.4 Zasady świadczenia usług Wsparcia Producenta

(1) Wykonawca zobowiązany jest zapewnić wsparcie producenta tych urządzeń (dalej określanego jako „**Producent**”) lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt II powyżej.

(2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.

(3) Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych.

Pozostałe wymagania zostały opisane w Projektowanych postanowieniach umowy, które zawarte są w rozdziale III SWZ.