ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI VI

I. Nazwa zamówienia

Zakup 8 wirtualnych appliance (klasy NGFW), 2 konsoli zarządzających wraz z usługami wsparcia na okres 36 miesięcy.

I.1 Kody CPV

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

II. Przedmiot zamówienia

(1) Przedmiotem zamówienia jest zakup licencji na witualny appliance klasy NGFW (ang. Next Generation Firewall) i konsoli zarządzających wraz z usługami wsparcia producenta dla licencji 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 NGFW, bieżących problemów dotyczących funkcjonowania NGFW, ich konfiguracji, wyjaśniania wątpliwości lub rozwiązania zagadnień z tego zakresu przedstawianych przez Zamawiającego, związanych z obsługą NGFW, świadczone w miejscu zainstalowania Urządzeń lub zdalnie, na warunkach wskazanych w OPZ i w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.
Godziny Robocze	oznacza godziny od 09:00 do 17:00 w dni od poniedziałku do piątku, nie będące dniami ustawowo wolnymi od pracy na terenie Rzeczypospolitej Polskiej.
Roboczogodzina	Jedna godzina pracy jednego członka personelu Wykonawcy.
Wsparcie producenta	Oznacza oferowane przez producenta NGFW aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych NGFW przez zdefiniowany okres czasu, zgodnie z pkt III.3 OPZ.
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)
Wirtualny Appliance	ang. Virtual Appliance oznacza oprogramowanie, do którego Producent dostarcza funckjonalności systemu klasy NGFW oraz wsparcie techniczne.

(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 przyapdkach) 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 zobwiązany jest posiadać status partnera producenta NGFW i Konsoli NGFW 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.

(10) 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

III.1 Dostawa licencji

(1) Przedmiotem zamówienia jest dostawa **8 licencji** na wirtualne systemy klasy NGFW (ang. Next Generation Firewall) zwane dalej „**NGFW**" i dostawa **2 licencji** na konsolę (wirtualny appliance) zarządzającą w/w NGFW, zwaną dalej **„Konsola NGFW**" zgodnie z poniższymi wymogami.

(2) Termin dostawy licencji wynosi do 5 Dni Roboczych od dnia zawarcia umowy;

Wymagania dla NGFW i konsoli NGFW		
LP.	**Opis wymagania**	**Parametry minimalne**
1.	Ogólne	1.1. NGFW i Konsola NGFW muszą pochodzić od tego samego producenta. 1.2. NGFW i Konsola NGFW 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. 1.3. NGFW powinien posiadać zgodność z profilem zabezpieczeń Common Criteria: „Stateful Traffic Filter Firewalls" lub równoważnym[1] (kryteriastosowane w celu oceny równoważności zostały opisane w rozdziale I SWZ); 1.4. NGFW powinien posiadać zgodność z profilem zabezpieczeń Common Criteria: "Virtual Private Network (VPN) Gateways lub równoważnym[2] (kryteria stosowane w celu oceny równoważności zostały opisane w rozdziale I SWZ); 1.5. NGFW lub Konsola NGFW muszą dostarczać mechanizm szyfrowania danych, który będzie posiadał certyfikat FIPS 140-2 lub FIPS 140-3 lub równoważny*

[1] Stanowi kryterium oceny ofert.
[2] Stanowi kryterium oceny ofert.

2.	Wirtualny Appliance	2.1. NGFW i konsola NGFW musi być dostarczona w postaci licencji niezbędnych do uruchomienia oprogramowania zgodnego z poniższymi wymaganiami na NGFW i konsole NGFW w formie Wirtualnego Appliance,przystosowanego do uruchomienia na co najmniej jednej z następujących platform wirtualizacji: VMWare lub KVM.

*Zamawiający wskazuje następujące kryteria stosowane w celu oceny równoważności dla normy FIPS 140-2 lub 140-3 i uzna za normę równoważną opisywanej, normę która:

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.1.1 Wymagania szczegółowe dla NGFW

LP.	Opis wymagania	Parametry minimalne
3.	Infrastruktura sieciowa	3.1. NGFW musi umożliwiać współpracę z systemami programowo sterowanych sieci (SDN) z co najmniej jednym z poniższych rozwiązań: • Cisco ACI lub • VMWare NSX-V lub • VMWare NSX-T
4.	Zarządzanie NGFW	4.1. Zarządzanie musi odbywać się z linii poleceń (CLI) oraz z konsoli GUI dostępnej przez WWW. 4.2. Musi pozwalać na zdefiniowanie min. 10 administratorów NGFW o różnych uprawnieniach. 4.3. Musi umożliwiać uwierzytelnianie administratorów za pomocą: • bazy lokalnej, • LDAP, • RADIUS 4.4. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co

		najmniej dwie metody uwierzytelniania (np. baza lokalna lub LDAP i RADIUS). 4.5. Interfejs administracyjny NGFW musi być w języku polskim lub angielskim. 4.6. Musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu NGFW bez użycia konsoli zarządzania lub linii poleceń (CLI). 4.7. Musi zapewniać możliwość zapisywania i odtworzenia (zapisanej wcześniej) konfiguracji. 4.8. Musi zapewniać, za pomocą konsoli GUI/CLI możliwość (niezależnie od zewnętrznej konsoli opisanej poniżej w tabeli „Wymagania szczegółowe dla Konsoli NGFW" w III.1.2 pkt 30-32 poniżej): 4.8.1. zarządzania konfiguracją NGFW. 4.8.2. zarządzania i konfiguracją (dodawanie i modyfikacja) polityk/reguł bezpieczeństwa zaimplementowanymi na NGFW. 4.8.3. monitorowania i szczegółowej analizy zarejestrowanych zdarzeń bezpieczeństwa w NGFW. 4.8.4. musi umożliwiać zbieranie i prezentowanie informacji dotyczących połączeń sieciowych przetwarzanych przez NGFW oraz zarejestrowanych zdarzeń bezpieczeństwa. Zbierane dane powinny zawierać informacje co najmniej o ruchu sieciowym, aplikacjach, zagrożeniach lub filtrowanych stronach WWW bez limitu licencyjnego na ilość przyjmowanych danych z NGFW (jedynym ograniczeniem może być ilość miejsca na dysku). 4.8.5. musi umożliwiać wysyłanie logów systemowych/audytowych, dotyczących monitorowania stanu NGFW oraz logów z zarejetrowanymi zdarzeniami

		bezpieczeństwa i połączeniami sieciowymi do systemów klasy SIEM.
5.	Przepustowość pojedynczego NGFW	5.1. NGFW musi zapewnić co najmniej poniższe parametry w zakresie wydajności: 5.1.1. przepustowość w trybie ochrony Firewall, IPS i kontroli aplikacji nie mniejsza niż 1 Gbps. 5.1.2. maksymalna ilość nowych sesji na sekundę nie mniejsza niż 10 000. 5.1.3. maksymalna ilość połączeń/sesji nie mniejsza niż 250 000. 5.1.4. maksymalna ilość równoległych sesji użytkowników SSL VPN nie mniejsza niż 100.
6.	Wymagania dot. trybu HA / klastra	6.1. NGFW musi mieć możliwość pracy w trybie High Availability lub klastra z drugą instancją NGFW - Active/Active i Active/Pasive.
7.	Tryb pracy	7.1. NGFW musi działać w co najmniej trzech trybach pracy: 7.1.1. jako przełącznik w drugiej warstwie modelu OSI (L2), 7.1.2. jako router w trzeciej warstwie modelu OSI (L3), 7.1.3. w trybie pasywnego nasłuchu (ruch ze SPAN/TAP - tryb IDS)
8.	IPv6	8.1. NGFW musi zapewniać obsługę protokołu IPv6.
9.	NAT	9.1. NGFW musi zapewniać statyczną i dynamiczną translację adresów NAT.
10.	DHCP	10.1. NGFW musi zapewniać usługę serwera DHCP i obsługę protokołu DHCP.
11.	VLAN	11.1. NGFW musi zapewniać obsługę protokół Ethernet z obsługą sieci VLAN. 11.2. Musi zapewniać obsługę łącz typu trunk z włączonym tagowaniem ramek, w standardzie IEEE 802.1Q.
12.	VPN	12.1. NGFW musi zapewniać możliwość zestawiania kryptograficznych tuneli IPSEC VPN typu site-to-site w oparciu o mechanizmy IPSec, IKE. 12.2. Zapewniać możliwość zestawienia tuneli VPN (SSL/TLS VPN) typu Remote Access z możliwością definiowania sieci wewnętrznych

		do których dostęp będzie dozwolony jak również sieci do których będzie blokowany. 12.3. Musi mieć możliwość tworzenia VPN-a typu (z obsługą IPv6) dla min. 100 kont pracujących równolegle. 12.4. Musi zapewniać możliwość uwierzytelniania użytkowników w oparciu o co najmniej następujące źródła: LDAP, lokalna baza danych.
13.	Zarządzanie pasmem (QoS)	13.1. NGFW musi zapewniać zarządzanie pasmem (QoS). 13.2. Musi umożliwić definiowanie parametrów ruchu sieciowego w oparciu o co najmniej następujące parametry: rozpoznany ruch sieciowy aplikacji oraz adresy IP (źródłowy i docelowy).
14.	Mechanizm ochrony DoS	14.1. NGFW musi zapewniać automatyczną ochronę przed atakami typu DoS z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 14.2. Ochrona przed atakami typu flood SYN/TCP.
15.	Polityki NGFW w module Firewall i IPS	15.1. NGFW musi zapewniać kontrolę ruchu sieciowego w oparciu o definiowane polityki. 15.2. Musi zapewniać kontrolę ruchu sieciowego w ramach polityk bezpieczeństwa i uwzględniać strefy bezpieczeństwa, adresy IP źródła i celu, protokoły i usługi sieciowe, aplikacje, kategorie URL/domen, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie QoS. 15.3. Musi zapewniać kontrolę/filtrację/inspekcję ruchu sieciowego na poziomie warstw L3-L7. 15.4. Musi zapewniać ochronę przed atakami wykorzystującymi fragmentację pakietów. 15.5. Musi zapewniać definiowanie polityk dostępu do zasobów w oparciu tożsamość użytkowników. 15.6. Musi zapewniać integracje z co najmniej następującymi źródłami tożsamości: MS Active Directory, LDAP. 15.7. 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); 15.8. Musi umożliwiać tworzenie polityk bezpieczeństwa w oparciu o mechanizmy geolokalizacji. Baza geolokalizacji musi być aktualizowana w sposób automatyczny (przez producenta NGFW).
16.	Klasyfikacja ruchu sieciowego	16.1. NGFW musi zapewniać rozpoznawanie ruchu sieciowego związanego z aplikacjami w oparciu o sygnatury, bez względu na użyte numery portów, protokoły tunelowania i szyfrowania. 16.2. Musi zapewniać rozpoznawanie ruchu sieciowego dla co najmniej 50 predefiniowanych aplikacji takich jak google drive, gmail, skype, P2P. 16.3. Musi zapewniać rozpoznawanie ruchu sieciowego dla predefiniowanych aplikacji w przypadku zastosowania tunelowania w oparciu o protokół HTTP lub HTTPS. 16.4. Musi umożliwiać tworzenie sygnatur dla nowych aplikacji bez użycia zewnętrznych narzędzi.
17.	Mechanizmy ochrony	17.1. NGFW musi zapewniać ochronę typu Firewall, IPS, AV/AM (ang. AntyVirus)/AntyMalware), identyfikacje aplikacji i kategoryzacje URL oraz domen.
18.	Mechanizm analizy plików (antymalware/antyspyreware)	18.1. NGFW musi zapewniać możliwość analizy przesyłanych plików w ruchu przychodzącym jak i wychodzącym. 18.2. Musi zapewniać możliwość rozpoznawanie typów pliku w oparciu o predefiniowane definicje uwzględniając w tym co najmniej pliki typu wykonywalnego PE32, pdf, MS Office, jpg, Java Script, svg. 18.3. Musi zapewniać ochronę przed atakami typu drive-by-download.

		18.4. Musi zapewniać możliwość blokowania transmisji plików na podstawie definicji typu plików. Rozpoznawanie typu pliku musi się odbywać w oparciu np. o nagłówek pliku i typ MIME bez względu na rozszerzenie.
19.	Mechanizm Web filtering	19.1. NGFW musi zapewniać możliwość definiowania reguł związanych z filtrowaniem URL (URL Filtering) oraz filtrowaniem WEB (ang. WEB Filtering). 19.2. Musi zapewniać filtrowanie w oparciu o kategorie (np. Adult, Gambling, Social Networking, video stream, Malware, Phishing, C&C, TOR, Proxy anonimizujące, itp.), przy czym producent dostarcza predefiniowany zestaw kategorii i przypisaną do nich bazę adresów URL i domen. Baza adresów musi być cyklicznie aktualizowania przez Producenta. 19.3. Musi zapewnić możliwość ręcznego definiowania dodatkowych kategorii bez użycia zewnętrznych narzędzi oraz możliwość przypisywanie do nich adresów URL i domen.
20.	Mechanizm IPS (Intrusion Prevention System)	20.1. NGFW musi zapewniać funkcjonalność Intrusion Prevention System (IPS) i Intrusion Detection System (IDS). 20.2. Baza sygnatur IPS/IDS musi być przechowywania na NGFW, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent NGFW. Aktualizacja bazy sygnatur musi być zapewniona w całym okresie wsparcia, o którym mowa w pkt III.3. poniżej (Zasady świadczenia usług wsparcia producenta). 20.3. Musi zapewniać możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa (Firewall). Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per cały system lub jego interfejs logiczny (np. interfejs sieciowy). 20.4. Musi zapewniać możliwość ręcznego tworzenia sygnatur IPS/IDS bezpośrednio na NGFW bez użycia zewnętrznych narzędzi.

		20.5. Musi zapewnić identyfikację ruchu sieciowego klasyfikowanego jako Command and Control.
21.	Mechanizm Antywirus / AntyMalware / Antyspareware	21.1. NGFW musi zapewniać funkcjonalność Antywirus/AntyMalware/Antyspareware (AV/AM). 21.2. Baza sygnatur AV/AM musi być przechowywania w NGFW, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent NGFW. Aktualizacja bazy sygnatur musi być zapewniona w całym okresie wsparcia, o którym mowa w pkt III.3 poniżej (dot. Zasad świadczenia usług wsparcia producenta). 21.3. Musi zapewniać możliwość uruchomienia Moduł AV/AM (ang. AntyVirus/ AntyMalware/ Antyspareware) per reguła polityki bezpieczeństwa. Nie jest dopuszczalne aby modułu inspekcji AV/AM uruchamiany był per cały system lub jego interfejs logiczny (sieciowy).
22.	Mechanizm przekierowywania plików do Sandbox-a	22.1. Musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych środowisk symulacyjnych (ang. „Sandbox") plików różnych typów (min.: pliki wykonywalne PE32, pdf, MS Office, Java Script, jpg) przechodzących w ruchu sieciowym chronionym przez NGFW.
23.	Mechanizmy analizy i blokowania DNS	23.1. NGFW musi umożliwiać wykrywanie i blokowanie ruchu sieciowego do domen uznanych za złośliwe i CnC.
24.	Mechanizmy dot. ruchu szyfrowanego	24.1. NGFW musi posiadać możliwość deszyfracji ruchu szyfrowanego HTTPS (HTTP szyfrowane w oparciu o protokół SSL/TLS) dla ruchu wychodzącego oraz wchodzącego. 24.2. Musi zapewnić możliwość definiowania reguł/polityk dla zdeszyfrowanego i szyfrowanego ruchu (w celu realizacji tzw. Security chain).
25.	Logowanie	25.1. Musi umożliwiać wysyłanie logów z informacjami o ruchu sieciowym chronionym

		przez NGFW do zewnętrznego systemu klasy SIEM. 25.2. Musi umożliwiać wysyłanie logów systemowych/audytowych, logów dotyczących stanu NGFW (monitorowanie wydajności i zużycia zasobów) oraz logów z zarejetrowanymi zdarzeniami bezpieczeństwa i połączeniami sieciowymi do systemów klasy SIEM.
26.	Mechanizmy zarządzania tożsamością użytkowników	26.1. NGFW musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: • Microsoft Active Directory lub • LDAP. 26.2. Musi umożliwiać wstawianie informacji o użytkowniku w nagłówkach protokołu http (np. X-Authenticated-User).
27.	Wsparcie dotyczące przepływów sieciowych (FLOW)	27.1. Musi zapewniać logowanie wszystkich przesyłanych pakietów (przepływów sieciowych) na wszystkich interfejsach NGFW. 27.2. Musi zapewniać możliwość konfiguracji eksportu tych danych do zewnętrznego systemu.
28.	Funkcjonalność dot. zapytań DNS	28.1. NGFW musi posiadać funkcjonalność weryfikacji i kontroli zapytań DNS. 28.2. Konieczna jest możliwość definiowania statycznych mapowań FQDN – IP i przekierowywania zapytań o wybrane domeny do wybranych serwerów DNS.
29.	Interfejsy	29.1. Musi umożliwić utworzenie min. dwa interfejsy logiczne (sieciowe/wirtualne).

III.1.2 Wymagania szczegółowe dla Konsoli NGFW

30.	Ogólne	30.1. Wraz z NGFW konieczne jest dostarczenie Konsoli NGFW pełniącej funkcje zarządzania w/w NGFW. 30.2. Konsola NGFW musi mieć możliwość podłączenia i zarządzania nie mniej niż 20 NGFW. 30.3. Musi zapewnić obsługę przestrzeni dyskowej o pojemności nie mniejszej niż 1 TB. 30.4. Musi posiadać możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczoną na logi. 30.5. Musi umożliwiać zbieranie i prezentowanie informacji dotyczących połączeń sieciowych przetwarzanych przez NGFW oraz zarejestrowanych zdarzeń bezpieczeństwa, bez limitu licencyjnego na ilość przyjmowanych danych z NGFW (jedynym ograniczeniem może być ilość miejsca na dysku). 30.6. Musi umożliwiać wysyłanie logów systemowych/audytowych, dotyczących monitorowania stanu NGFW oraz logów z zarejetrowanymi zdarzeniami bezpieczeństwa i połączeniami sieciowymi do systemów klasy SIEM.
31.	Analiza danych	31.1. Musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji/danych pochodzących z NFGW w tym co najmniej umożliwiać: 31.1.1. tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 31.1.2. tworzenie statycznych raportów dopasowanych do aktualnych potrzeb. 31.1.3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail.

		31.1.4. możliwość szczegółowych analiz bezpieczeństwa z z funkcjonalnością „drill-down” – analizy od ogółu do szczegółu. 31.1.5. Nie może być limitu licencyjnego na ilość danych pozyskiwanych z NGFW.
32.	Zarządzanie	32.1. Musi umożliwiać zarządzanie NGFW w tym co najmniej: 32.1.1. budowanie i dystrybucję polityk bezpieczeństwa NGFW. 32.1.2. umożliwiać grupowanie zarządzanych NGFW logiczne grupy NGFW umożliwiające wspólne zarządzanie (np.: konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, aktualizowanie wersji oprogramowania). 32.1.3. pozwalać na tworzenie raportów na podstawie zbudowanych grup logicznych NGFW. 32.1.4. umożliwiać zarządzanie obiektami używanymi przez wszystkie zarządzane NGFW. 32.2. Musi umożliwiać zarządzaniem konfiguracjami w tym co najmniej: 32.2.1. umożliwiać dystrybucję i zdalną instalację nowych wersji system. 32.2.2. umożliwiać tworzenie kopii zapasowych zarządzanych NGFW. 32.2.3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur. 32.2.4. umożliwiać audytowanie/ sprawdzanie poprawności (monitoring typu health check) działania NGFW. 32.2.5. informować o zmianach konfiguracji systemu. 32.3. Musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do NGFW. 32.4. Musi umożliwiać uwierzytelnianie administratorów za pomocą co najmniej: bazy lokalnej, LDAP, RADIUS.

		32.5. Musi pozwolić na pracę przez min. 30 użytkowników (administratorów i użytkowników zarządzających NGFW przy założeniu, że będą pracować na konsoli NGFW równolegle.

III.2 Zasady realizowania Godzin eksperckich w ramach prawa opcji

(1) Zamawiający wymaga zapewnienia przez Wykonawcę Godzin eksperckich świadczonych przez autoryzowany podmiot współpracujący bezpośrednio z producentem przedmiotu zamówienia opisanego w pkt III.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 (dalej określanego jako „**Partner**") – w wymiarze łącznie 696 Roboczogodzin, przez okres od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.1 powyżej do końca grudnia 2022r.

(2) Osoba/y realizująca Godziny eksperckie musi być ekspertem w obszarze związanym z technologią dot. przedmiotu zamówienia (**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 Godzin eksperckich będzie m.in.:

(a) opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt III.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 błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

(c) wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.1 powyżej,

(d) konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez NGFW stanowiące przedmiot zamówienia, o którym mowa w pkt III.1 powyżej,

(e) przygotowanie i przeprowadzenie Instruktażu w zakresie korzystania z NGFW oraz Konsoli NGFW, w taki sposób, aby każda z osób uczestniczących w instruktażu posiadała wiedzę i umiejętności potrzebne do prawidłowej obsługi i samodzielnej konfiguracji NGFW oraz Konsoli NGFW, z wykorzystaniem jego wszystkich funkcjonalności. Zamawiający będzie wymagał przeprowadzenia takiego instruktażu przez co najmniej jedną osobę, która w okresie dwóch lat przed realizacją instruktażu ukończyła szkolenie oferowane przez producenta NGFW oraz Konsoli NGFW, w zakresie objętym instruktażem oraz legitymuje się certyfikatem potwierdzającym ukończenie takiego szkolenia.

(4) Zamawiający wymaga zapewnienia realizacji Godzin eksperckich, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej wykonawca 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.

III.3 Zasady świadczenia usług wsparcia producenta

(1) Wykonawca zobowiązany jest zapewnić wsparcie Producenta NGFW i konsoli NGFW (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 (dalej określanego jako „Partner"), dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt III.1.

(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 w trybie 24/7/365.

(4) Podjęcie reakcji na zgłoszenie serwisowe będzie nastepować w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.