OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa przedmiotu zamówienia:

Dostawa subskrypcji wraz z zapewnieniem usług wsparcia technicznego oraz usługami godzin eksperckich dla 8 Wirtualnych Appliance (klasy NGFW) oraz 2 konsoli zarządzających na okres 12 miesięcy.

2. Oznaczenie przedmiotu zamówienia wg Kod CPV:

48730000-4 – Pakiety oprogramowania zabezpieczającego
72611000-6 Usługi w zakresie wsparcia technicznego.
72250000-2 Usługi w zakresie konserwacji i wsparcia systemów.

3. Definicje:

Wszelkie pojęcia opisane w OPZ należy rozumieć zgodnie z ich definicją tam zawartą. Ponadto Opis Przedmiotu Zamówienia (dalej: „OPZ") wprowadza dodatkowe pojęcia, które pisane wielką literą należy czytać zgodnie z ich definicją:

L.p.	Termin	Definicja
1.	**Aktualizacje**	Uaktualnienia Oprogramowania, nowe wersje Oprogramowania (upgrade), niższe wersje Oprogramowania (downgrade), wydania uzupełniające, poprawki programistyczne (patche), nowe wydania Oprogramowania będące kontynuacją linii produktowej, poprawki, w tym bezpieczeństwa, definicje, sygnatury, nowe wydania Oprogramowania oraz inne dostosowania zapewniające prawidłowe korzystanie z Oprogramowania.
2.	**Awaria**	Nieprawidłowe działanie Oprogramowania, w szczególności brak możliwości używania Oprogramowania zgodnie z przeznaczeniem lub dokumentacją Producenta.
3.	**Dni Robocze**	Dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.
4.	**Godziny eksperckie**	Usługi konsultacyjne opisane w pkt 9 OPZ.
5.	**Godziny Robocze**	Godziny od 9:00 do 17:00 w Dni Robocze.
6.	**Lokalizacja**	Dwa miejsca na terenie miasta stołecznego Warszawy, w których będą świadczone usługi Gwarancji, Wsparcia Technicznego, Godziny eksperckie. Dokładne adresy zostaną podane do wiadomości Wykonawcy po podpisaniu Umowy.
6.	**Oprogramowanie**	Całość lub dowolny element Oprogramowania opisanego w pkt 6 w Tabeli nr 1 OPZ lub równoważne.
7.	**Opcja**	Uprawnienie Zamawiającego do rozszerzenia zakresu zamówienia o prace w ramach Godzin eksperckich, szczegółowo opisane w pkt 9 OPZ. Przedmiotowe uprawnienie będzie realizowane każdorazowo na Zlecenie Zamawiającego.
8.	**Producent**	Producent Oprogramowania/Subskrypcji.
9.	**Protokół odbioru**	Dokument potwierdzający przekazanie Zamawiającemu wszystkich wymaganych materiałów i dokumentów opisanych w OPZ.
10.	**Roboczogodzina**	Jednostka miary czasu świadczenia Godzin eksperckich, obejmująca pracę jednej osoby przez 1 godzinę zegarową, do której nie wlicza się czasu dojazdu do lokalizacji, w której usługa jest wykonywana.

11.	**Subskrypcja/Licencja**	Uprawnienie do zgodnego z prawem korzystania z Oprogramowania i jego Aktualizacji, elementów Wsparcia Technicznego lub innego prawa udzielanego w celu wykonania Umowy, na warunkach wskazanych przez Producenta Oprogramowania oraz na warunkach wskazanych w Umowie.
12.	**Wirtualny Appliance**	ang. Virtual Appliance oznacza oprogramowanie, do którego Producent dostarcza funkcjonalności systemu klasy NGFW oraz Wsparcie Techniczne.
13.	**Wsparcie Techniczne**	Świadczenie przez Wykonawcę usług Wsparcia technicznego Oprogramowania na warunkach opisanych w OPZ.
14.	**Zgłoszenie**	Poinformowanie przez Zamawiającego Wykonawcy o wystąpieniu Awarii. Poinformowanie o wystąpieniu Awarii poprzez kanał wskazany w pkt 5.3.6 OPZ. Za chwilę dokonania Zgłoszenia Strony uznają datę i godzinę poinformowania przez Zamawiającego o wystąpieniu Awarii. W przypadku dokonania Zgłoszenia przez więcej niż jeden kanał, chwilą dokonania Zgłoszenia będzie wcześniejsza data i godzina.
15.	**Zlecenie**	Dokument w formie pisemnej (w tym w formie elektronicznej, opatrzonej ważnym kwalifikowanym podpisem elektronicznym), na podstawie którego Zamawiający powierzy Wykonawcy wykonywanie Godzin eksperckich, wskazujący zakres oraz terminy prac, które Wykonawca zobowiązuje się wykonywać jako Godziny eksperckie, sporządzony zgodnie ze wzorem, stanowiącym **Błąd! Nie można odnaleźć źródła odwołania.** do Umowy.

4. Przedmiot zamówienia:

4.1. Dostawa Subskrypcji dla Oprogramowania wraz ze Wsparciem Technicznym na okres 12 miesięcy;
4.2. Zapewnienie świadczenia usług 120 Godzin eksperckich w ramach Opcji.

5. Terminy realizacji:

5.1. Wykonawca zobowiązany będzie zapewnić dostawę Subskrypcji dla Oprogramowania, Wsparcie Techniczne w terminie do 5 Dni Roboczych od dnia zawarcia Umowy przez okres 12 miesięcy od dnia odbioru, wskazanego w podpisanym przez Strony Protokole Odbioru.
5.2. Wykonawca zobowiązany będzie zapewnić możliwość realizacji Godzin eksperckich, przez okres 12 miesięcy od dnia odbioru, wskazanego w podpisanym przez Strony Protokole Odbioru.
5.3. Wykonawca w ciągu 5 Dni Roboczych od dnia zawarcia Umowy zobowiązuje się dostarczyć Zamawiającemu na adres e-mail wskazany w Umowie, dane dostępowe i dokumenty:
   5.3.1. wszystkie wymagane klucze licencyjne i aktywacyjne (w przypadku oprogramowania Równoważnego);
   5.3.2. certyfikat lub inny dokument Producenta potwierdzający dostawę Subskrypcji dla Oprogramowania;
   5.3.3. dokument potwierdzający objęcie Oprogramowania Wsparciem Technicznym wraz ze wskazaniem okresu obowiązywania;
   5.3.4. dokumentację, w szczególności umowę licencyjną, zawierającą warunki licencjonowania danego Oprogramowania określone przez Producenta, o ile dokumentacja taka nie została udostępniona na portalu Producenta;
   5.3.5. aktualne zestawienie w formacie XLS/XLSX/pdf wszystkich pozycji Oprogramowania objętych Wsparciem Technicznym, zawierające informacje: m.in. oznaczenie katalogowe produktu Producenta (tzw. part number), pełna nazwa produktu, okres obowiązywania Wsparcia Technicznego oraz ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto;
   5.3.6. adresy poczty elektronicznej, numery telefonów oraz dane dostępowe do portalu klienckiego, umożliwiające Zamawiającemu skorzystanie ze Wsparcia Technicznego (w przypadku oprogramowania Równoważnego).

6. Specyfikacja posiadanego przez Zamawiającego Oprogramowania:

W chwili obecnej, Zamawiający posiada wymienione w Tabeli nr 1 produkty, które są objęte wsparciem technicznym Producenta.

Tabela nr 1 Wykaz Oprogramowania.

L.p.	Nazwa (opis licencji / subskrypcji)	Kod producenta	Poziom wsparcia technicznego	Ilość
1.	Cisco Firepower FTD Virtual Base Lic, 3 Gbps	FTD-V-20SBSE-K9 lub równoważny	24/7	8
2.	Cisco Firepower FTD Virtual TP, Malware & URL Lic, 3 Gbps	FTD-V-20STMC lub równoważny	24/7	8
3.	Cisco AnyConnect VPN Only, 100 Simultaneo us (eDelivery)	L-AC-VPNO100= lub równoważny	24/7	8
4.	Cisco Firepower Management Center, (VMWare) for 300 devices	SF-FMC-VMW-300- K9 lub równoważny	24/7	2

7. Ogólne warunki realizacji przedmiotu zamówienia:

7.1. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży na rzecz Skarbu Państwa – Ministra Cyfryzacji.

7.2. Licencjobiorcą i właścicielem Oprogramowania jest Skarb Państwa - Minister Cyfryzacji. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego użytkownika Oprogramowania jakim będzie Skarb Państwa - Minister Cyfryzacji, z adresem korespondencyjnym przy ul. Królewskiej 27, 00-060 Warszawa, NIP 525-295-50-37, REGON 525189465. Zamawiający kupuje przedmiot zamówienia na potrzeby Skarbu Państwa - Ministra Cyfryzacji.

7.3. Zamawiający wymaga, aby Wykonawca posiadał status partnera Producenta Oprogramowania na terenie Polski. Zamawiający wyklucza sytuację, w której wyłącznie podwykonawca posiada status, o którym mowa w zdaniu powyżej.

7.4. Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 5 ust 1 pkt 4 lit. d w zw. z art. 4 pkt. 1 Ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r. poz. 20 ze zm.), dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, Oprogramowanie musi być zgodne z obowiązującymi przepisami prawa w zakresie cyberbezpieczeństwa, w tym z Ustawą o krajowym systemie cyberbezpieczeństwa, oraz że jego wykorzystanie nie będzie powodować powstania nieuzasadnionych zagrożeń dla cyberbezpieczeństwa, bezpieczeństwa publicznego ani istotnych interesów bezpieczeństwa państwa.

7.5. Wykonawca oświadcza, że jest świadomy, iż z uwagi na wymogi bezpieczeństwa obowiązujące w Lokalizacji, osoby wyznaczone przez Wykonawcę do realizacji Umowy mogą być zobowiązane do okazania służbom ochrony obiektów, przed rozpoczęciem realizacji przedmiotu Umowy w danej Lokalizacji, poświadczenia bezpieczeństwa dostępu do informacji niejawnych na poziomie min. „POUFNE”.

7.6. Wykonawca zobowiązany jest zapewnić Zamawiającemu dostawę Subskrypcji wyszczególnionych w pkt. 6 Tabela 1 lub równoważne pochodzących z legalnego kanału dystrybucji.

7.7. Wszystkie dostarczone Subskrypcje muszą pozwalać na swobodne przenoszenie pomiędzy urządzeniami (np. w przypadku wymiany urządzenia).

7.8. Wszelkie dostarczane Subskrypcje muszą posiadać pełną funkcjonalność dla produktów określonych w Tabeli nr 1 zgodnie z dokumentacją Producenta.

8. Warunki realizacji usług Wsparcia Technicznego:

8.1. Wykonawca zobowiązany jest zapewnić Zamawiającemu Wsparcie Techniczne dla Oprogramowania realizowane przez Producenta bezpośrednio lub przez autoryzowany podmiot współpracujący z Producentem w języku polskim lub angielskim.

8.2. W ramach Wsparcia Technicznego dla Oprogramowania, Zamawiający ma:

8.2.1. prawo do dokonywania Zgłoszeń Awarii w trybie 24/7/365, za pośrednictwem telefonu lub dedykowanej aplikacji lub adresu poczty elektronicznej, wskazanych przez Wykonawcę;

8.2.2. prawo do wydawanych przez Producenta najnowszych wersji, Aktualizacji Oprogramowania oraz poprawek do Oprogramowania;

8.2.3. dostęp elektroniczny przez 24 godziny na dobę, 7 dni w tygodniu do pomocy technicznej;

8.2.4. dostęp elektroniczny do bazy wiedzy, dokumentacji, biuletynów i informacji na temat Oprogramowania i urządzeń, posiadanych produktów;

8.3. Szczegółowe warunki Wsparcia Technicznego dla Oprogramowania regulują warunki Producenta Oprogramowania, z zastrzeżeniem, że nie mogą być mniej korzystne niż warunki wskazane w OPZ lub Umowie.

9. Warunki realizacji usługi Godzin eksperckich w ramach Opcji:

9.1. Zamawiający jest uprawniony do zlecania Wykonawcy w ramach Opcji świadczenia usługi Godzin eksperckich, świadczonej przez inżyniera certyfikowanego przez Producenta Oprogramowania, w miejscu zainstalowania Oprogramowania lub zdalnie – zgodnie ze Zleceniem Zamawiającego - realizowanej w Dni robocze, w godzinach od 9:00 do 17:00 w maksymalnym wymiarze 120 Roboczogodzin.

9.2. W ramach usług realizowanych jako Godziny eksperckie będą m.in. wykonywane na Zlecenie Zamawiającego:

9.2.1. Konsultacje i wsparcie w zakresie rozbudowy, tuningu i Oprogramowania;

9.2.2. Warsztaty i szkolenia w zakresie przedmiotu zamówienia dla pracowników Zamawiającego;

9.2.3. Opracowanie i dostarczenie dokumentów, procedur i instrukcji, dot. m.in.:

9.2.3.1. instalacji, konfiguracji oraz parametryzacji przedmiotu zamówienia;

9.2.3.2. Aktualizacji i wdrażania poprawek do przedmiotu zamówienia;

9.2.4. Wsparcie Zamawiającego w użytkowaniu przedmiotu zamówienia – zarówno techniczne, jak i merytoryczne oraz w zakresie implementacji nowych funkcjonalności lub modyfikacji już skonfigurowanych.

9.2.5. Wsparcie Zamawiającego w planowanych pracach serwisowych obejmujących przeprowadzenie:

9.2.5.1. standardowych prac serwisowych;

9.2.5.2. Aktualizacji;

9.2.5.3. weryfikacji poprawności konfiguracji.

9.3. W zakresie przedmiotu Opcji, rozliczenie wynagrodzenia Wykonawcy będzie następować w oparciu o stawkę godzinową pracy konsultanta, w ramach wskazanej puli Roboczogodzin na zasadach opisanych w OPZ i Umowie.
9.4. Zlecenie w zakresie skorzystania z Opcji następować będzie na zasadach określonych w OPZ.
9.5. Skorzystanie z Opcji jest uprawnieniem Zamawiającego. Zamawiający nie zobowiązuje się w żaden sposób do skorzystania z Opcji. Nieskorzystanie przez Zamawiającego w całości lub w części z tego prawa nie rodzi po stronie Wykonawcy jakichkolwiek roszczeń w stosunku do Zamawiającego.
9.6. Na wniosek Zamawiającego, usługa Godzin eksperckich zostanie przeprowadzona w trybie online. Wykonawca zobowiązany jest zapewnić wszelkie niezbędne narzędzia do przeprowadzenia usługi online, w tym odpowiednią platformę. Do czasu trwania usługi online nie wlicza się czasu, kiedy nie mogła być ona prowadzona z przyczyn leżących po stronie Wykonawcy lub z powodów technicznych, np. zakłócenia połączenia, awaria sprzętu lub oprogramowania.

10. Opis rozwiązania równoważnego

10.1. Zamawiający wskazuje, że zgodnie z przepisem art. 99 ust. 6 PZP dokonał opisu przedmiotu zamówienia poprzez wskazanie produktu referencyjnego oraz określenie następujących kryteriów stosowane w celu oceny równoważności. Produkt opisany powyżej jako przedmiot zamówienia (produkt referencyjny) jest rozwiązaniem aktualnie wykorzystywanym przez Zamawiającego, skonfigurowanym do współpracy z innymi rozwiązaniami informatycznymi wykorzystywanymi przez Zamawiającego, które zostały dobrane i skonfigurowane do pracy z produktem referencyjnym. Zamawiający uzna przedmiot oferty za równoważny, jeżeli na podstawie treści oferty i dołączonych do niej przedmiotowych środków dowodowych, wykonawca wykaże, że przedmiot zamówienia zostanie wykonany z zachowaniem następujących zasad:

10.1.1. Produkt referencyjny, jest wdrożony i skonfigurowany do współpracy z utrzymywanymi przez Zamawiającego Systemami, realizującymi usługi publiczne prowadzone przez Ministra Cyfryzacji (dalej określanymi jako „Systemy") i w związku z tym Zamawiający wymaga, aby wdrożenie produktu równoważnego zapewniało ciągłość działania tych Systemów (przy dopuszczeniu okna serwisowego o zakresie adekwatnym dla danego Systemu) poprzez zapewnienie, że:

10.1.1.1. przed rozpoczęciem realizacji dostaw produktów równoważnych, Wykonawca zobowiąże się przedstawić zakres oraz treść zmian konfiguracyjnych, jakie należy wprowadzić w tych systemach, dla zapewnienia, iż zostaną zachowane ich wszystkie funkcjonalności, zapewnione aktualnie poprzez wykorzystanie produktu referencyjnego (Zamawiający zobowiązuje się udostępniać Wykonawcy informacje dotyczące bieżącej konfiguracji i funkcjonalności systemów, w oparciu o takie same zasady dotyczące zakresu dostępu oraz obowiązku zachowania poufności jakie dotyczą wszystkich innych wykonawców, którym dane takie są udostępniane w celu wykonywania zamówień publicznych);

10.1.1.2. po zaakceptowaniu zakresu takich prac przez Zamawiającego, Wykonawca zobowiąże się odwzorować środowisko produkcyjne, na którym działają Systemy oraz przeprowadzenia w nim wszystkich testów, jakie zostały przeprowadzone na tych Systemach przed ich produkcyjnym wdrożeniem przez Zamawiającego – w tym testów penetracyjnych, wykonanych przez podmiot zewnętrzny, niezależny od Wykonawcy – oraz zademonstrować Zamawiającemu działanie tak przygotowanego środowiska testowego (Zamawiający zobowiązuje się udostępniać Wykonawcy możliwość korzystania z kopii

Systemów do celów testowych, w oparciu o takie same zasady dotyczące zakresu dostępu oraz obowiązku zachowania poufności jakie dotyczą wszystkich innych wykonawców, którym dane takie są udostępniane w celu wykonywania zamówień publicznych). Zamawiający wymaga, aby wszystkie komponenty środowiska testowego zostały zainstalowane przez Wykonawcę we wskazanej przez Zamawiającego lokalizacji oraz skonfigurowane z pozostałymi elementami sieciowymi Zamawiającego, w przez Wykonawcę we wskazanej przez Zamawiającego lokalizacji oraz skonfigurowane z pozostałymi elementami sieciowymi Zamawiającego, w celu przeprowadzenia testów. Dane testowe, odpowiadające charakterystyce danych rzeczywistych wykorzystywanych w Systemach zostaną dostarczone przez Zamawiającego, na potrzeby testów.

10.1.1.3. po zaakceptowaniu przez Zamawiającego wyników testów przeprowadzonych w środowisku testowym Wykonawcy, Wykonawca zobowiąże się przedstawić Zamawiającemu projekt haromonogramu wdrożenia produktu równoważnego, uwzględniający zakres oraz terminy szkoleń i instruktażu stanowiskowego, dla personelu Zamawiającego, który korzystał z produktu referencyjnego, o zakresie zapewniającym Zamawiającemu zachowanie ciągłości działania Systemów. Wykonawca zobowiązany będzie przenieść na zamawiającego wszystkie autorskie prawa majątkowe do oprogramowania wytworzonego w celu wykonania wdrożenia.

10.2. W sytuacji, w której wdrożenie produktu równoważnego nie będzie możliwe przed dniem zakończenia wsparcia technicznego wykupionego przez Zamawiającego dla aktualnie wykorzystywanego przez niego rozwiązania referencyjnego – Wykonawca wykonujący wdrożenie produktu równoważnego będzie zobowiązany do zapewnienia przedłużenia takiego wsparcia technicznego do czasu wdrożenia produkcyjnego rozwiązania równoważnego.

10.3. Zamawiający nie uznaje, aby produktem równoważnym był produkt, którego wykorzystanie nakłada na Zamawiającego obowiązek ponownego poniesienia kosztów finansowych, w tym kosztów Systemów korzystających z rozwiązania równoważnego oraz organizacyjnych, a także ryzyk, które już zostały poniesione dla zbudowania aktualnie funkcjonujących Systemów, zintegrowanych z produktem referencyjnym i w związku z tym wymaga, aby zostały one uwzględnione w cenie produktu równoważnego.

10.4. Zamawiający wymaga, aby wszystkie funkcjonalności produktu równoważnego były dostępne od dnia uruchomienia środowiska testowego, a po wdrożeniu produktu równoważnego, wraz ze wsparciem technicznym, w okresach wskazanych w OPZ dla produktu referencyjnego, poczynając od dnia wdrożenia.

10.5. W opisie przedmiotu zamówienia Zamawiający w zakresie każdego wskazania wymienionego w poniższym punkcie Wymagania funkcjonalne dla oprogramowania równoważnego wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania rozwiązania równoważnego, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne wszystkich kryteriów równoważności.

10.6. 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.

10.7. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne 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.

11. Kryteria stosowane w celu oceny równoważności

11.1. Wymagania ogólne dla NGFW i konsoli NGFW (oprogramowanie równoważne)

11.1.1. NGFW i Konsola NGFW muszą pochodzić od tego samego producenta.
11.1.2. 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 rozwiązania zostanie zakończone przed rokiem 2027.
11.1.3. NGFW musi posiadać zgodność z profilem zabezpieczeń Common Criteria: „Stateful Traffic Filter Firewalls" lub równoważnym.
11.1.4. NGFW musi posiadać zgodność z profilem zabezpieczeń Common Criteria: "Virtual Private Network (VPN) Gateways lub równoważnym.
11.1.5. NGFW lub Konsola NGFW muszą dostarczać mechanizm szyfrowania danych, który będzie posiadał certyfikat FIPS 140-2 lub FIPS 140-3 lub równoważny.
11.1.6. 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 z następujących typach obrazów: OVA, ISO, QCOW/QCOW2.
11.1.7. 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:
11.1.7.1. Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
11.1.7.2. Została wydana 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,
11.1.7.3. Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
11.1.7.4. 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.

11.2. Wymagania szczegółowe dla NGFW

11.2.1. NGFW musi zapewniać współpracę z systemami programowo sterowanych sieci (SDN) z co najmniej jednym z poniższych rozwiązań:
11.2.1.1. Cisco ACI lub
11.2.1.2. VMWare NSX-V lub
11.2.1.3. VMWare NSX-T
11.2.2. Zarządzanie musi odbywać się z linii poleceń (CLI) oraz z konsoli GUI dostępnej przez WWW.
11.2.3. Musi pozwalać na zdefiniowanie min. 10 administratorów NGFW o różnych uprawnieniach.
11.2.4. Musi zapewniać uwierzytelnianie administratorów za pomocą:
11.2.4.1. bazy lokalnej,
11.2.4.2. LDAP,
11.2.4.3. RADIUS.

11.2.5. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej dwie metody uwierzytelniania (np. baza lokalna lub LDAP i RADIUS).
11.2.6. Interfejs administracyjny NGFW musi być w języku polskim lub angielskim.
11.2.7. 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).
11.2.8. Musi zapewniać możliwość zapisywania i odtworzenia (zapisanej wcześniej) konfiguracji.
11.2.9. Musi zapewniać, za pomocą konsoli GUI/CLI możliwość:
11.2.9.1. zarządzania konfiguracją NGFW.
11.2.9.2. zarządzania i konfiguracją (dodawanie i modyfikacja) polityk/reguł bezpieczeństwa zaimplementowanymi na NGFW.
11.2.9.3. monitorowania i szczegółowej analizy zarejestrowanych zdarzeń bezpieczeństwa w NGFW musi zapewniać 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).
11.2.9.4. musi zapewniać wysyłanie logów systemowych/audytowych, dotyczących monitorowania stanu NGFW oraz logów z zarejestrowanymi zdarzeniami.
11.2.10. NGFW musi zapewnić co najmniej poniższe parametry w zakresie wydajności:
11.2.10.1. przepustowość w trybie ochrony Firewall, IPS i kontroli aplikacji nie mniejsza niż 1 Gbps.
11.2.10.2. maksymalna ilość nowych sesji na sekundę nie mniejsza niż 10 000.
11.2.10.3. maksymalna ilość połączeń/sesji nie mniejsza niż 250 000.
11.2.10.4. maksymalna ilość równoległych sesji użytkowników SSL VPN nie mniejsza niż 100
11.2.11. NGFW musi mieć możliwość pracy w trybie High Availability lub klastra z drugą instancją NGFW - Active/Active i Active/Pasive.
11.2.12. NGFW musi działać w co najmniej trzech trybach pracy:
11.2.12.1. jako przełącznik w drugiej warstwie modelu OSI (L2),
11.2.12.2. router w trzeciej warstwie modelu OSI (L3),
11.2.12.3. w trybie pasywnego nasłuchu (ruch ze SPAN/TAP - tryb IDS).
11.2.13. NGFW musi zapewniać obsługę protokołu IPv6.
11.2.14. NGFW musi zapewniać statyczną i dynamiczną translację adresów NAT.
11.2.15. NGFW musi zapewniać usługę serwera DHCP i obsługę protokołu DHCP
11.2.16. NGFW musi zapewniać obsługę protokół Ethernet z obsługą sieci VLAN.
11.2.17. Musi zapewniać obsługę łącz typu trunk z włączonym tagowaniem ramek, w standardzie IEEE 802.1Q.
11.2.18. NGFW musi zapewniać możliwość zestawiania kryptograficznych tuneli IPSEC VPN typu site-to-site w oparciu na mechanizmach IPSec, IKE.
11.2.19. Musi zapewniać możliwość zestawienia tuneli VPN (SSL/TLS VPN) typu Remote Access z możliwością definiowania sieci wewnętrznych Strona 7 z 15 do których dostęp będzie dozwolony jak również sieci do których będzie blokowany.
11.2.20. Musi mieć możliwość tworzenia VPN-a typu (z obsługą IPv6) dla min. 100 kont pracujących równolegle.
11.2.21. Musi zapewniać możliwość uwierzytelniania użytkowników w oparciu o co najmniej następujące źródła: LDAP, lokalna baza danych.
11.2.22. NGFW musi zapewniać zarządzanie pasmem (QoS).
11.2.23. Musi zapewniać definiowanie parametrów ruchu sieciowego w oparciu o co najmniej następujące parametry: rozpoznany ruch sieciowy aplikacji oraz adresy IP (źródłowy i docelowy).

11.2.24. NGFW musi zapewniać automatyczną ochronę przed atakami typu DoS z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
11.2.25. Ochrona przed atakami typu flood SYN/TCP.
11.2.26. NGFW musi zapewniać kontrolę ruchu sieciowego w oparciu o definiowane polityki.
11.2.27. 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.
11.2.28. Musi zapewniać kontrolę/filtrację/inspekcję ruchu sieciowego na poziomie warstw L3-L7.
11.2.29. Musi zapewniać ochronę przed atakami wykorzystującymi fragmentację pakietów.
11.2.30. Musi zapewniać definiowanie polityk dostępu do zasobów w oparciu tożsamość użytkowników.
11.2.31. Musi zapewniać integracje z co najmniej następującymi źródłami tożsamości:
  11.2.31.1. MS Active Directory,
  11.2.31.2. LDAP.
11.2.32. Musi zapewniać blokowania ruchu sieciowego na podstawie:
  11.2.32.1. adresów IP (w tym Original Client IP z pola XFF);
  11.2.32.2. reputacji (IP, domen lub URL);
  11.2.32.3. sygnatur IPS;
  11.2.32.4. Domen;
  11.2.32.5. URL;
  11.2.32.6. Geolokalizacji (np. adresy IP pochodzących z konkretnych państw);
11.2.33. Musi zapewniać tworzenie polityk bezpieczeństwa w oparciu na mechanizmie geolokalizacji. Baza geolokalizacji musi być aktualizowana w sposób automatyczny (przez producenta NGFW).
11.2.34. NGFW musi zapewniać rozpoznawanie ruchu sieciowego związanego z aplikacjami w oparciu na sygnaturach, bez względu na użyte numery portów, protokoły tunelowania i szyfrowania.
11.2.35. Musi zapewniać rozpoznawanie ruchu sieciowego dla co najmniej 50 predefiniowanych aplikacji takich, jak: google drive, gmail, skype, P2P.
11.2.36. Musi zapewniać rozpoznawanie ruchu sieciowego dla predefiniowanych aplikacji w przypadku zastosowania tunelowania w oparciu o protokół HTTP lub HTTPS.
11.2.37. Musi zapewniać tworzenie sygnatur dla nowych aplikacji bez użycia zewnętrznych narzędzi.
11.2.38. NGFW musi zapewniać możliwość analizy przesyłanych plików w ruchu przychodzącym jak i wychodzącym.
11.2.39. 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.
11.2.40. Musi zapewniać ochronę przed atakami typu drive-by-download.
11.2.41. Musi zapewniać możliwość blokowania transmisji plików na podstawie definicji typu plików. Rozpoznawanie typu pliku musi się odbywać w oparciu np. na nagłówku pliku i typ MIME bez względu na rozszerzenie.
11.2.42. NGFW musi zapewniać możliwość definiowania reguł związanych z filtrowaniem URL (URL Filtering) oraz filtrowaniem WEB (ang. WEB Filtering).
11.2.43. Musi zapewniać filtrowanie w oparciu na kategoriach (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.
11.2.44. Musi zapewnić możliwość ręcznego definiowania dodatkowych kategorii bez użycia zewnętrznych narzędzi oraz możliwość przypisywanie do nich adresów URL i domen
11.2.45. NGFW musi zapewniać funkcjonalność Intrusion Prevention System (IPS) i Intrusion Detection System (IDS).

11.2.46. 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.
11.2.47. 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).
11.2.48. Musi zapewniać możliwość ręcznego tworzenia sygnatur IPS/IDS bezpośrednio na NGFW bez użycia zewnętrznych narzędzi.
11.2.49. Musi zapewnić identyfikację ruchu sieciowego klasyfikowanego jako Command and Control.
11.2.50. NGFW musi zapewniać funkcjonalność Antywirus/AntyMalware/Antyspareware (AV/AM).
11.2.51. 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.
11.2.52. 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).
11.2.53. Musi zapewniać 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
11.2.54. NGFW musi zapewniać wykrywanie i blokowanie ruchu sieciowego do domen uznanych za złośliwe i CnC.
11.2.55. NGFW musi zapewniać możliwość deszyfracji ruchu szyfrowanego HTTPS (HTTP szyfrowane w oparciu o protokół SSL/TLS) dla ruchu wychodzącego oraz wchodzącego.
11.2.56. Musi zapewnić możliwość definiowania reguł/polityk dla zdeszyfrowanego i szyfrowanego ruchu (w celu realizacji tzw. Security chain).
11.2.57. Musi zapewniać wysyłanie logów z informacjami o ruchu sieciowym chronionym przez NGFW do zewnętrznego systemu klasy SIEM.
11.2.58. Musi zapewniać wysyłanie logów systemowych/audytowych, logów dotyczących stanu NGFW (monitorowanie wydajności i zużycia zasobów) oraz logów z zarejestrowanymi zdarzeniami bezpieczeństwa i połączeniami sieciowymi do systemów klasy SIEM.
11.2.59. NGFW musi zapewniać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu na:
    11.2.59.1. Microsoft Active Directory lub LDAP.
    11.2.59.2. Musi zapewniać wstawianie informacji o użytkowniku w nagłówkach protokołu http (np. X-Authenticated-User).
11.2.60. Musi zapewniać logowanie wszystkich przesyłanych pakietów (przepływów sieciowych) na wszystkich interfejsach NGFW.
11.2.61. Musi zapewniać możliwość konfiguracji eksportu tych danych do zewnętrznego systemu.
11.2.62. NGFW musi posiadać funkcjonalność weryfikacji i kontroli zapytań DNS.
11.2.63. Musi posiadać możliwość definiowania statycznych mapowań FQDN – IP i przekierowywania zapytań o wybrane domeny do wybranych serwerów DNS.
11.2.64. Musi umożliwić utworzenie min. dwa interfejsy logiczne (sieciowe/wirtualne).
11.2.65. NGFW musi umożliwiać (konfiguracyjnie i licencyjnie) prace w trybie HA (Active/Standby).

11.3. Wymagania dla Konsoli NGFW

11.3.1. Wraz z NGFW konieczne jest dostarczenie Konsoli NGFW pełniącej funkcje zarządzania w/w NGFW.
11.3.2. Konsola NGFW musi umożliwiać (konfiguracyjnie i licencyjnie) prace w trybie HA (Active/Standby).
11.3.3. Konsola NGFW musi zapewniać możliwość podłączenia i zarządzania nie mniej niż 20 NGFW.
11.3.4. Musi zapewnić obsługę przestrzeni dyskowej i licencyjna (na logi) o pojemności nie mniejszej niż 1 TB (w tym logi: audytowe, dot. przetwarzanego ruchu sieciowego, zarejestrowanych zdarzeń bezpieczeństwa).
11.3.5. Musi posiadać możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczoną na logi.
11.3.6. Musi zapewniać 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).
11.3.7. Musi zapewniać wysyłanie logów systemowych/audytowych, dotyczących monitorowania stanu NGFW oraz logów z zarejestrowanymi zdarzeniami bezpieczeństwa i połączeniami sieciowymi do systemów klasy SIEM.
11.3.8. Musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji/danych pochodzących z NFGW w tym co najmniej umożliwiać:
11.3.8.1. tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
11.3.8.2. tworzenie statycznych raportów dopasowanych do aktualnych potrzeb.
11.3.8.3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail.
11.3.8.4. możliwość szczegółowych analiz bezpieczeństwa z funkcjonalnością „drill-down" – analizy od ogółu do szczegółu.
11.3.8.5. Nie może być limitu licencyjnego na ilość danych pozyskiwanych z NGFW.
11.3.9. Musi umożliwiać zarządzanie NGFW w tym co najmniej:
11.3.9.1. budowanie i dystrybucję polityk bezpieczeństwa NGFW.
11.3.9.2. umożliwiać grupowanie zarządzanych NGFW logiczne grupy NGFW umożliwiające wspólne zarządzanie (np.: konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, aktualizowanie wersji oprogramowania).
11.3.9.3. pozwalać na tworzenie raportów na podstawie zbudowanych grup logicznych NGFW.
11.3.9.4. umożliwiać zarządzanie obiektami używanymi przez wszystkie zarządzane NGFW.
11.3.10. Musi umożliwiać zarządzaniem konfiguracjami w tym co najmniej:
11.3.10.1. umożliwiać dystrybucję i zdalną instalację nowych wersji system.
11.3.10.2. umożliwiać tworzenie kopii zapasowych zarządzanych NGFW.
11.3.10.3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur.
11.3.10.4. umożliwiać audytowanie/ sprawdzanie poprawności (monitoring typu health check) działania NGFW.
11.3.10.5. informować o zmianach konfiguracji systemu.
11.3.11. Musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do NGFW.
11.3.12. Musi umożliwiać uwierzytelnianie administratorów za pomocą co najmniej: bazy lokalnej, LDAP, RADIUS.
11.3.12. Musi pozwolić na pracę przez min. 30 użytkowników (administratorów i użytkowników zarządzających NGFW przy założeniu, że będą pracować na konsoli NGFW równolegle.

Pozostałe wymagania opisane zostały w Projektowanych postanowieniach umowy (zawartych w rozdziale III SWZ).