Opis Przedmiotu Zamówienia (OPZ)

**I. PRZEDMIOT ZAMÓWIENIA I WYMAGANIA OGÓLNE**

Przedmiotem zamówienia jest:

1. Dostawa trzech klastrów urządzeń do zabezpieczenia ruchu sieciowego w postaci rozwiązań Next Generation Firewall (dalej: firewall lub NGFW).
2. Dostawa i rozbudowa komponentu zarządczego.
3. Przeprowadzenie analizy przedwdrożeniowej, wdrożenie i uruchomienie systemu zabezpieczeń NGFW.
4. Realizacja szkoleń autoryzowanych przez producenta oferowanego sprzętu.
5. Realizacja wsparcia technicznego i licencji na niezbędne do funkcjonowania elementy przez okres 60 miesięcy od daty zakupu.

**TABELA NR 1:**

| **Lp.** | **NAZWA SPRZĘTU** | **ILOŚĆ** |
| --- | --- | --- |
| **PCK** | **SWP** | **CEY** | **RAZEM** |
| 1 | Urządzenia NGFW typu A (w konfiguracji klastra HA) | **2** | **0** | **0** | **2** |
| 2 | Licencje i subskrypcje (w tym m.in. dostęp VPN) dla wymaganych funkcjonalności na okres co najmniej 60 miesięcy dla zaoferowanych urządzeń NGFW typu A | **2** | **0** | **0** | **2** |
| 3 | Aktywne wsparcie techniczne opisane wymaganiami zamówienia na okres co najmniej 60 miesięcy dla zaoferowanych urządzeń typ A | **2** | **0** | **0** | **2** |
| 4 | Urządzenia NGFW typu B (w konfiguracji klastra HA) | **0** | **2** | **2** | **4** |
| 5 | Licencje i subskrypcje (w tym m.in. dostęp VPN) dla wymaganych funkcjonalności na okres co najmniej 60 miesięcy dla zaoferowanych urządzeń NGFW typu B | **0** | **2** | **2** | **4** |
| 6 | Aktywne wsparcie techniczne opisane wymaganiami zamówienia na okres co najmniej 60 miesięcy dla zaoferowanych urządzeń typ B | **0** | **2** | **2** | **4** |
| 7 | Analiza przedwdrożeniowa, wdrożenie i szkolenia dla personelu | **1** |
| 8 | Przedłużenie wsparcia technicznego dla obecnego u Zamawiającego systemu zarządzania centralnego (SZC) Palo Alto Panorama VM na okres 60 miesięcy na poziomie wsparcia co najmniej Partner Enabled Premium Support | **1** |
| 9 | Serwerowe dyski twarde do rozbudowy serwera systemowego zarządzania centralnego (SZC) Palo Alto Panorama VM | **4** |

Nazewnictwo placówek:

PCK – Szpital Morski im. PCK w Gdyni

SWP – Szpital św. Wincentego a Paulo w Gdyni

CEY – Szpital Specjalistyczny w Wejherowie

Termin realizacji zamówienia: do **30 dni** od daty podpisania umowy.

Wykonawca wystawi odpowiedni dowód sprzedaży (fakturę VAT) w odpowiednim terminie wynikającym z umowy.

# WYMAGANIA OGÓLNE

1. W niniejszym dokumencie przedstawiono minimalne parametry urządzeń. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna. Wartości te należy zawsze rozumieć jako ograniczone z bezsporną korzyścią dla Zamawiającego.
2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producenta.
3. Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowa, wcześniej nieużywana.
4. Urządzenia muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji.
5. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim. Wersja angielska dopuszczalna jest w przypadku braku dostępności wersji polskiej dokumentacji.
6. Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe, szyny i elementy montażowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
7. Oferowany sprzęt musi posiadać oznakowanie CE.
8. Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia urządzenia w EOL (brak wsparcia producenta lub wycofanie urządzenia z oficjalnej dystrybucji).
9. Wszystkie zestawy komputerowe, laptopy, drukarki oraz sprzęt zasilany przez zasilacze pośrednie muszą współpracować z siecią energetyczną o parametrach: 230V±10%, 50Hz.

**II. NIETECHNICZNE CECHY URZĄDZEŃ**

1. Przedmiot zamówienia musi być fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu, spełniający normy CE. Nie dopuszcza się urządzeń typu refurbished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
2. Zamawiający wymaga, aby wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.
3. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania.
4. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) - na dzień składania oferty.

**III. DODATKOWE SYSTEMY ZEWNĘTRZNE**

Zamawiający dopuszcza, aby całościowy system bezpieczeństwa był zbudowany w oparciu o wymagane komponenty opisane w OPZ wraz z elementami dodatkowymi, których zastosowanie jest opcjonalne, ale mające na celu zrealizowanie wdrożenia. Decyzja o ich zastosowaniu leży w gestii Wykonawcy - jeżeli uzna on na etapie analizy przedwdrożeniowej wspólnie z Zamawiającym, iż dla osiągnięcia opisanych wymagań niezbędne są dodatkowe systemy zewnętrzne to Zamawiający zezwala na ich zastosowanie pod warunkami opisanymi poniżej:

1. Stosowanie dodatkowych systemów nie może dotyczyć funkcji ochronnych NGFW (np. wykrywania aplikacji, obsługi IPS, AV czy NAT).
2. Stosowanie dodatkowych systemów nie może powodować ominięcia reguł bezpieczeństwa. Przykładowo stosowanie dodatkowych systemów jest dopuszczalne, gdy są one konieczne np. dla:
3. weryfikacji tożsamości użytkowników – system uwierzytelniania;
4. realizacji funkcji zarządzania firewallem i uprawnieniami administratorów;
5. zatwierdzania zmian w konfiguracji;
6. realizacji funkcji inspekcji ruchu SSL;
7. realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania.
8. Systemy wspomagające muszą być zaoferowane w pełnym wsparciem producenta, co oznacza wymóg zaoferowania wszystkich pakietów serwisowych dostępnych dla danego rozwiązania.
9. W przypadku stosowania systemów wspomagających Zamawiający wymaga aby były one oferowane przez tego samego producenta co oferowany system firewall i całościowo serwisowane przez tego producenta.
10. Stosowanie dodatkowych systemów jest możliwe tylko przy założeniu zapewnienia ich wysokiej dostępności i niezawodności (HA). Oznacza to, że należy dostarczyć każdy taki system jako dedykowane rozwiązanie (urządzenie z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta); system musi być dostarczony jako klaster niezawodnościowy – tzn. identyczne urządzenia pracujące równolegle w modelu 1+1 lub N+1. Dodatkowe systemy muszą zostać zaoferowane w konfiguracji sprzętowej „analogicznej” dla konfiguracji urządzeń NGFW.
11. Zamawiający wymaga również, aby wszystkie dostarczane systemy wspomagające były sprawdzone w praktyce rynkowej i spełniały wymagania w tym obszarze analogicznie do firewalli, oznacza to, iż oprogramowanie systemowe realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.
12. Zapewnienie redundancji nie jest wymagane dla usług realizowanych z chmury Threat Intelligence producenta oferowanego rozwiązania.

**IV. WYMAGANIA OGÓLNE DLA NGFW TYPU A – 1 KOMPLET (2 SZTUKI), URZĄDZENIA PRACUJĄCE W KLASTRZE NIEZAWODNOŚCIOWYM W PLACÓWCE SZPITALNEJ W LOKALIZACJI W GDYNI**

1. Firewalle muszą być dostarczone w postaci dedykowanych rozwiązań sprzętowo-programowych (tzw. appliance).
2. Cechy wydajnościowe:
	1. 15Gbps przepustowości firewall/kontroli aplikacji;
	2. 9Gbps przepustowości firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
	3. 9Gbps dla IPsec VPN;
	4. 1.800.000 jednoczesnych sesji;
	5. 200.000 nowych połączeń na sekundę;
	6. 1.800 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
	7. 10 wirtualnych routerów posiadających odrębne tabele routingu;
	8. Możliwość licencyjnej rozbudowy do 10 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji - polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.
	9. 150 stref bezpieczeństwa;
	10. Lokalna przestrzeń pamięci co najmniej o pojemności 400GB przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi).
3. Cechy urządzenia – interfejsy, zasilanie:
	1. Wysokość maksymalnie 2U wraz z zestawem montażowym do szafy RACK 19”;
	2. dwa redundantne zasilacze AC 230V Hot-Swap z kompletami kabli;
	3. 10 portów 10-GigabitEthernet RJ45 (dopuszcza się uzyskanie tych portów poprzez zastosowanie portów 10 GigabitEthernet SFP+ obsadzonych modułami z RJ45, natomiast nie dopuszcza się wykorzystania do tego celu portów wymienionych w pkt 3d);
	4. 10 portów 10 GigabitEthernet SFP+ obsługujących moduły optyczne SR oraz LR;
	5. 4 porty 25 GigabitEthernet SFP28;
	6. 1 port 1 GigabitEthernet RJ45 lub 10 GigabitEthernet RJ45 wyłącznie do celów zarządzania (dopuszcza się uzyskanie tego portu poprzez zastosowanie portów SFP/SFP+ obsadzonych modułami z RJ45, natomiast nie dopuszcza się wykorzystania do tego celu portów wymienionych w pozostałych punktach);
	7. Urządzenie musi posiadać dedykowany/wydzielony port 2,5G lub 5G lub 10 GigabitEthernet lub szybszy dla celów połączenia urządzeń w klaster (high availability). Port ten musi być traktowany jako dodatkowy względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach powyżej.
4. Wymagania funkcjonalne dla rozwiązań NGFW Typu A

UWAGA: Wszystkie wymienione poniżej funkcje muszą być dostępne i realizowane przez firewall jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenie lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego.

Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.

1. Cechy NGFW.
2. Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. NFGW musi wykrywać co najmniej 4000 aplikacji predefiniowanych przez Producenta.
3. Transparentne ustalenie tożsamości użytkowników.
4. Realizowanie funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:
	1. Intrusion Prevention System (IPS),
	2. Antywirus (AV),
	3. Anty-Spyware / Anty-Malware,
	4. Kategoryzacja URL i filtracja URL,
	5. Ochrona DNS,
	6. Sandbox lokalny lub chmurowy tego samego producenta.
5. Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory.
6. System musi zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
7. Silniki detekcyjne i ochronne NGFW.
8. Bazy sygnatur IPS, AV, Anty-Spyware (lub innego silnika, jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, regularnie aktualizowane w sposób automatyczny.
9. Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.
10. Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
11. Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa. Nie dopuszcza się by IPS i AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego, gdzie administrator nie ma możliwości konfiguracji jaka część ruchu będzie podlegała inspekcji i w jakim zakresie.
12. Wykrywanie aktywności sieci typu Botnet.
13. Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office w tym zawierających makra, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
14. Funkcja filtrowania ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron:
	1. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp.);
	2. Ocena strony musi obejmować określenie ryzyka do niej przypisanego (co najmniej wysokie-średnie-niskie);
	3. Musi być zapewniona możliwość tworzenia własnych list stron (whitelist oraz blacklist) bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta z możliwością konfiguracji, gdzie własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.
15. Funkcja ochrony przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem:
	1. Możliwość przesyłania do systemu sandbox (tego samego producenta co firewall) plików zdefiniowanych przez administratora (co najmniej exe, dll, java, MS Office w tym zawierających makra, pdf). Zamawiający dopuszcza by odbywało się̨ to poprzez dedykowany mechanizm wbudowany w urządzenie lub przez jeden z wymaganych silników detekcyjnych, przy czym funkcja ta musi mieć możliwość wskazania/wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno kierunku transmisji (ruch wchodzący/wychodzący ze wskazanej strefy bezpieczeństwa), adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy.
	2. Możliwość aktualizacji systemu firewall o nowo wykryte (w sandbox) zagrożenia. Aktualizacje muszą być dystrybuowane niezwłocznie i na bieżąco, to znaczy bezpośrednio po ich wykryciu przez producenta. Nie jest dopuszczalne aby aktualizacje systemu firewall odbywały się w trybie regularnych uaktualnień publikowanych przez producenta np. co 24 godziny.
	3. Administrator musi posiadać dostęp do raportów z sandboxa dotyczących plików wysyłanych przez urządzenia, jak również posiadać możliwość manualnego wysłania pliku (np. poprzez upload przez stronę www) do sandboxa.
	4. Dopuszcza się zarówno realizację sandboxa w postaci chmury producenta jak i rozwiązania lokalnego. W tym drugim przypadku wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanym firewallem.
	5. Bez względu na użyte rozwiązanie, wymaga się wydajności zapewniającej jednoczesną analizę minimum 20 plików/próbek w tzw. VM Sandboxing (rozumiana jako realizacja funkcjonalności sandbox polegająca na wykorzystaniu instancji maszyn wirtualnych z określonymi systemami operacyjnymi i zestawem zainstalowanych aplikacji do zdetonowania/uruchomienia, a następnie analizy podejrzanego pliku pod kątem jego potencjalnie negatywnego wpływu na komputery klienckie lub serwery).
	6. Jednoczesna analiza 20 próbek/plików musi być zapewniona bez względu na to czy pliki te będą wysyłane automatycznie przez firewall czy manualnie przez administratora czy też będzie to mieszana grupa plików pochodząca zarówno bezpośrednio z firewalla, jak też od administratorów.
16. Podstawowa ochrona DNS co najmniej w zakresie:
	1. Wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 10 milionów wpisów.
	2. Możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing).
17. Deszyfracja ruchu.

Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS. Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3. Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:

* + 1. Realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 3 Gbps inspekcji TLS dla sesji http 64K;
		2. Jest wyposażone w co najmniej 4 interfejsy 10 GigabitEthernet SFP+;
		3. Zapewnia redundancję zasilaczy analogicznie do urządzeń firewall;
		4. Musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewalla;
		5. Musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewalla;.
		6. W przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.
1. Obsługa VPN oraz funkcji sieciowych.
	1. Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
	2. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN.
	3. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW - obsługa co najmniej 1800 tuneli/użytkowników.
	4. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS, Linux, Android i iOS.
	5. Oprogramowanie klienta VPN dla Windows i MacOS musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej co najmniej w zakresie sprawdzenia:
		1. czy zainstalowano oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury,
		2. czy włączony jest osobisty firewall,
		3. czy włączone jest szyfrowanie dysku.
	6. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewalla.
2. Wymagane jest zestawienie tuneli bez konieczności zastosowania klienta VPN - tzw. praca w trybie Clientless VPN – dla co najmniej 200 tuneli.
3. Jeżeli oprogramowanie klienta jest dodatkowo licencjonowane przez producenta wówczas należy przewidzieć je dla 2000 użytkowników/urządzeń oraz zapewnić możliwość licencyjnej rozbudowy do 5000.
4. Obsługa protokołów routingu: OSPFv2 i OSPFv3, BGP4.
5. Obsługa 4094 VLAN zgodnych z 802.1q.
6. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
7. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
8. Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
9. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
10. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).
11. Uwierzytelnienie i ustalanie tożsamości użytkowników.
12. Transparentne ustalenie tożsamości w oparciu o:
	1. integrację z kontrolerem domeny Active Directory;
	2. integrację z serwerami LDAP;
	3. integrację z serwerami terminalowymi;
	4. integrację bazującą na informacji z logów SYSLOG lub RADIUS pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX;
13. Firewall musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń;
14. Uwierzytelnianie administratorów NGFW za pomocą:
	1. bazy lokalnej;
	2. zewnętrznej usługi katalogowej dostępnej po LDAPS;
	3. RADIUS lub TACACS+.
15. Zarządzenie urządzeniami NGFW.
16. Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez Interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora - bez konieczności korzystania z centralnych narzędzi zarządzania.
17. Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
18. Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian (m.in. polityk, konfiguracji interfejsów, routingu itp.), ze wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

**V. WYMAGANIA OGÓLNE DLA NGFW TYPU B – 2 KOMPLETY (4 SZTUKI), URZĄDZENIA PRACUJĄCE W KLASTRZE NIEZAWODNOŚCIOWYM DLA PLACÓWEK SZPITALNYCH W LOKALIZACJI: W GDYNI ORAZ W WEJHEROWIE**

1. Firewalle muszą być dostarczone w postaci dedykowanych rozwiązań sprzętowo-programowych (tzw. appliance).
2. Cechy wydajnościowe:
	1. 8Gbps przepustowości Firewall/kontroli aplikacji;
	2. 4Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
	3. 4Gbps dla IPsec VPN;
	4. 750.000 jednoczesnych sesji;
	5. 50.000 nowych połączeń na sekundę;
	6. 1.500 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
	7. 5 wirtualnych routerów posiadających odrębne tabele routingu;
	8. Możliwość licencyjnej rozbudowy do 5 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu;
	9. 50 stref bezpieczeństwa;
	10. Lokalna przestrzeń pamięci co najmniej o pojemności 100GB przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi).
3. Cechy urządzenia – interfejsy, zasilanie:
	1. Wysokość maksymalnie 2U wraz z zestawem montażowym do szafy RACK 19”;
	2. 12 portów 1-GigabitEthernet RJ45 (dopuszcza się uzyskanie tych portów poprzez zastosowanie portów 1 GigabitEthernet SFP obsadzonych modułami z RJ45;
	3. 4 porty 1 GigabitEthernet SFP;
	4. 4 porty 10 GigabitEthernet SFP+ obsługujące moduły optyczne SR oraz LR;
	5. 1 port 1 GigabitEthernet RJ45 lub 10-GigabitEthernet RJ45 wyłącznie do celów zarządzania (dopuszcza się uzyskanie tego portu poprzez zastosowanie portów SFP/SFP+ obsadzonych modułami z RJ45);
	6. Urządzenie musi posiadać dedykowany/wydzielony port 2,5/5/10-GigabitEthernet (lub szybszy) dla celów połączenia urządzeń w klaster (high availability). Port ten musi być traktowany jako dodatkowy względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach powyżej.
4. Wymagania funkcjonalne dla rozwiązań NGFW dla NGFW Typu B.

UWAGA: Wszystkie wymienione poniżej funkcje muszą być dostępne i realizowane przez firewall jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenie lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego.

Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.

* + 1. Cechy NGFW.
1. Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. NFGW musi wykrywać co najmniej 4000 aplikacji predefiniowanych przez Producenta.
2. Transparentne ustalenie tożsamości użytkowników
3. Realizowanie funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:
	1. Intrusion Prevention System (IPS);
	2. Antywirus (AV);
	3. Anty-Spyware / Anty-Malware;
	4. Kategoryzacja URL i filtracja URL;
	5. Ochrona DNS;
	6. sandbox lokalny lub chmurowy tego samego producenta.
4. Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory.
5. System musi zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
	* 1. Silniki detekcyjne i ochronne NGFW.
6. Bazy sygnatur IPS, AV, Anty-Spyware (lub innego silnika, jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, regularnie aktualizowane w sposób automatyczny.
7. Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.
8. Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
9. Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa. Nie dopuszcza się by IPS i AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego, gdzie administrator nie ma możliwości konfiguracji jaka część ruchu będzie podlegała inspekcji i w jakim zakresie.
10. Wykrywanie aktywności sieci typu Botnet.
11. Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office (w tym zawierające makra), rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
12. Funkcja filtrowania ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron:
	1. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp.);
	2. Ocena strony musi obejmować określenie ryzyka do niej przypisanego (co najmniej wysokie-średnie-niskie);
	3. Musi być zapewniona możliwość tworzenia własnych list stron (whitelist oraz blacklist) bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta z możliwością konfiguracji, gdzie własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.
13. Funkcja ochrony przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem:
	1. Możliwość przesyłania do systemu sandbox (tego samego producenta co firewall) plików zdefiniowanych przez administratora (co najmniej exe, dll, java, MS Office (w tym zawierające makra), pdf). Zamawiający dopuszcza by odbywało się̨ to poprzez dedykowany mechanizm wbudowany w urządzenie lub przez jeden z wymaganych silników detekcyjnych przy czym funkcja ta musi mieć możliwość wskazania/wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno kierunku transmisji (ruch wchodzący/wychodzący ze wskazanej strefy bezpieczeństwa), adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy;
	2. Możliwość aktualizacji systemu firewall o nowo wykryte (w sandbox) zagrożenia. Aktualizacje muszą być dystrybuowane niezwłocznie i na bieżąco, to znaczy bezpośrednio po ich wykryciu przez producenta. Nie jest dopuszczalne, aby aktualizacje systemu związane z nowo wykrytymi zagrożeniami firewall odbywały się dopiero w trybie regularnych uaktualnień publikowanych przez producenta np. co 24 godziny;
	3. Administrator musi posiadać dostęp do raportów z sandboxa dotyczących plików wysyłanych przez urządzenia, jak również posiadać możliwość manualnego wysłania pliku (np. poprzez upload przez stronę www) do sandboxa;
	4. Dopuszcza się zarówno realizację sandboxa w postaci chmury producenta jak i rozwiązania lokalnego. W tym drugim przypadku wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanym firewallem;
	5. Bez względu na użyte rozwiązanie, wymaga się wydajności zapewniającej jednoczesną analizę minimum 10 plików/próbek w tzw. VM Sandboxing (rozumiana jako realizacja funkcjonalności sandbox polegająca na wykorzystaniu instancji maszyn wirtualnych z określonymi systemami operacyjnymi i zestawem zainstalowanych aplikacji do zdetonowania/uruchomienia, a następnie analizy podejrzanego pliku pod kątem jego potencjalnie negatywnego wpływu na komputery klienckie lub serwery);
	6. Jednoczesna analiza 10 próbek/plików w tzw. VM Sandboxing musi być zapewniona bez względu na to czy pliki te będą wysyłane automatycznie przez firewall czy manualnie przez administratora czy też będzie to mieszana grupa plików pochodząca zarówno bezpośrednio z firewalla, jak też od administratorów.
14. Podstawowa ochrona DNS co najmniej w zakresie:
	1. wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 10 milionów wpisów.
	2. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
		1. Deszyfracja ruchu.
15. Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do urządzenia NGFW, w celu jego dalszego przetwarzania. Urządzenie NGFW musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS). Dopuszcza się rozwiązanie zewnętrzne współpracujące z urządzeniem NGFW przy spełnieniu poniższych wymagań:
	* 1. Realizuje wymaganą funkcjonalność dla wydajności przetwarzania minimum 1Gbps inspekcji TLS dla sesji http 64K,
		2. Jest wyposażone w co najmniej 2 interfejsy 10 GigabitEthernet SFP+;
		3. Musi być dostarczone w modelu redundancji 1:1 (analogicznie do urządzeń firewall) z potrzebnymi licencjami i gwarancją/wsparciem zgodnym z długością wsparcia firewalla;
		4. Musi być dostarczone z potrzebnymi licencjami i gwarancją zgodną z długością wsparcia firewalla;
		5. W przypadku zewnętrznego urządzenia lub urządzeń innych niż NGFW wymagane jest dostarczenie opisu współpracy proponowanej integracji z NGFW wykonującym inspekcję wykrywania i zapobiegania włamaniom na rozszyfrowanym ruchu przez zewnętrzne urządzenia.
		6. Obsługa VPN oraz funkcji sieciowych.
16. Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
17. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN:
	1. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW- obsługa co najmniej 1500 tuneli/użytkowników;
	2. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows i MacOS;
	3. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewalla;
	4. Jeżeli oprogramowanie klienta jest dodatkowo licencjonowane przez producenta wówczas należy przewidzieć je dla 1500 użytkowników/urządzeń oraz zapewnić możliwość licencyjnej rozbudowy do 2000.
18. Obsługa protokołów routingu: OSPFv2 i OSPFv3, BGP4.
19. Obsługa 4094 VLAN zgodnych z 802.1q.
20. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
21. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
22. Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
23. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
24. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).
	* 1. Uwierzytelnienie i ustalanie tożsamości użytkowników.
25. Transparentne ustalenie tożsamości w oparciu o:
	1. integrację z kontrolerem domeny Active Directory;
	2. integracji z serwerami LDAP;
	3. integracji z serwerami terminalowymi;
	4. integracji bazującej na informacji z logów SYSLOG lub RADIUS pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX.
26. Firewall musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.
27. Uwierzytelnianie administratorów NGFW za pomocą:
	1. bazy lokalnej;
	2. zewnętrznej usługi katalogowej dostępnej po LDAPS;
	3. RADIUS lub TACACS+.
		1. Zarządzenie urządzeniami NGFW.
28. Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez Interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora - bez konieczności korzystania z centralnych narzędzi zarządzania.
29. Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
30. Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian (m.in. polityk, konfiguracji interfejsów, routingu itp.), ze wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

**VI. INTERPRETACJA PARAMETRÓW WYDAJNOŚCIOWYCH NGFW TYPU A I B**

1. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji - rozwiązanie pozwoli na:
	1. wykrycie aplikacji,
	2. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
2. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware - rozwiązanie pozwoli na
	1. wykrycie aplikacji,
	2. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych,
	3. inspekcje IPS całego ruchu,
	4. inspekcję antywirusową całego ruchu,
	5. inspekcję antymalware/AntySpyware całego ruchu,
	6. przesyłanie plików do sandboxa lokalnego i/lub chmurowego,
	7. przechwytywanie i blokowanie plików określonego typu.
	8. Logowanie zdarzeń

Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch - sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

**VII. SPECYFIKACJA KOMPONENTU ZARZĄDCZEGO**

Z racji, iż Zamawiający dysponuje systemem zarządzania centralnego (SZC) pod nazwą Panorama VM firmy Palo Alto Networks dla 25 urządzeń fizycznych, Zamawiający dopuszcza, aby w przypadku oferowania firewalli Palo Alto Networks system zarządzania centralnego (SCZ) nie był uwzględniony w ofercie. Jednocześnie Zamawiający wymaga, aby w takim przypadku częścią oferty było zapewnienie wsparcia serwisowego dla posiadanego systemu Panorama VM na okres **minimum 60 miesięcy**.

Wykonawca dostarczy również w ramach realizowanego zamówienia co najmniej 4 komplety serwerowych dysków twardych do serwera zarzadzania i logów Panorama VM w konfiguracji:

Rozmiar kieszeni dysku SSD: 2.5"

Pojemność pamięci SSD: 6,4TB

Standardowe rozwiązania komunikacyjne: SAS

Typ pamięci: TLC

NVMe: Nie

Przeznaczenie: Serwer/stacja robocza

Szyfrowanie sprzętu: Nie

Docelowe obciążenie pracą: Mixed Use (MU)

Szybkość przesyłania danych: 12Gbit/s

Prędkość odczytu z nośnika: 1080MB/s

Prędkość zapisu nośnika: 1030MB/s

Losowy odczyt (4KB): 105000 IOPS

Losowy zapis (4KB): 120000 IOPS

Opóźnienie odczytu: 195 µs

Opóźnienie zapisu: 95 µs

Obsługa podłączania podczas pracy: Tak

Preferowany dysk: HPE 6.4TB SAS 12G Mixed Use SFF (2.5in) Smart Carrier Multi Vendor SSD [Part number: P49056-B21]

W przypadku zastosowania rozwiązania innego producenta konieczne jest dostarczenie i wdrożenie zgodnie z ustaleniami z Zamawiającym podczas prowadzonej analizy przedwdrożeniowej systemu zarządzania i logowania (SZC) spełniającego poniższe wymagania:

1. Komponent zarządczy musi być dostarczony w postaci maszyny wirtualnej (virtual appliance) działającej w środowisku VMware ESXi.
2. Komponent zarządczy musi pochodzić od tego samego producenta, co urządzenia NGFW wchodzące w skład komponentu zabezpieczającego.
3. Komponent zarządczy musi umożliwiać zarządzanie łącznie co najmniej 10 fizycznymi urządzeniami NGFW i co najmniej 50 firewallami wirtualnymi rozumianymi jako wirtualny firewalli/system/domena/kontekst.
4. Zamawiający dopuszcza możliwość zastąpienia WebGUI, wyłącznie w momencie gdy:
5. zapewni wszystkie niezbędne licencje i komponenty, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie Zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc., Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę;
6. rozwiązanie to będzie umożliwiało dostęp dla co najmniej 10 osób jednocześnie;
7. gwarancja i wsparcie na rozwiązanie zastępujące WebGUI musi trwać cały okres gwarancyjny komponentu zabezpieczającego.
8. Komponent zarządczy musi umożliwiać zdefiniowanie co najmniej 10 lokalnych kont administracyjnych z możliwością określenia praw dostępu.
9. Komponent zarządczy musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
	1. Zarządza obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium;
	2. Zapewnia dystrybucję i zdalną instalację nowych sygnatur oraz wersji oprogramowania systemowego;
	3. Przechowuje różne wersje konfiguracji zarządzanych NGFW;
	4. Pozwala na tworzenie raportów na podstawie zbudowanych grup NGFW.
10. Komponent zarządczy musi dawać możliwość zbierania logów (dzienników zdarzeń) z zarządzanych urządzeń, ze wszystkimi ich funkcjami składowymi.
	1. Zbiera logi zdarzeń z oferowanych NGFW co najmniej o ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW;
	2. Umożliwia korelację logów zdarzeń z zarządzanych firewalli;
	3. Umożliwia tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych NGFW;
	4. Pozwala na tworzenie raportów na podstawie gromadzonych w logach informacji;
	5. Pozwala na zapisywanie stworzonych raportów, uruchamianie ich w sposób manualny lub automatyczny w określonych przedziałach czasu oraz eksport do formatu tekstowego.
11. Komponent zarządczy musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
12. Graficzny interfejs Komponentu Zarządczego (Web GUI) musi być dostępny po protokole HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii Java czy Flash.
13. Komponent zarządczy powinien pozwalać na obsługę co najmniej:
	1. Logi użytkowników:
		1. 5000 logów na sekundę;
		2. Przyrost dzienny nie mniej niż 150GB;
		3. 16TB użytecznej przestrzeni dyskowej;
		4. Retencja danych nie mniej niż 100 dni.
	2. Logi administracyjne:
		1. 100 logów na sekundę;
		2. Przyrost dzienny nie mniej niż 2GB;
		3. 4TB użytecznej przestrzeni dyskowej;
		4. Logi administracyjne przechowywane przez okres minimum 36 miesięcy.
14. Komponent zarządczy może zostać zbudowany w oparciu o dwie osobne maszyny wirtualne pochodzące od tego samego producenta (i jednocześnie producenta komponentu zabezpieczającego), współpracujące pomiędzy sobą, gdzie:
	1. Jedna maszyna jest dedykowana dla centralnego logowania zdarzeń i raportowania, obsługująca logi inspekcyjne.
	2. Druga maszyna jest dedykowana dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne.
	3. Obie maszyny (jako każda z osobna) muszą spełniać wymagania w zakresie:
		1. liczby zarządzanych firewalli;
		2. liczby docelowo zarządzanych firewalli;
		3. możliwości pracy autonomicznej, w szczególności nie dopuszcza się, aby spełnienie wymagań odbywało się przez współdzielenie zasobów przez poszczególne maszyny (awaria pojedynczej maszyny nie może wpływać na drugą). Dlatego też wymagane jest spełnienie wymagań do obu maszyn niezależnie. Do oferty należy dołączyć dodatkową dokumentację potwierdzającą spełnienie tych wymagań.
	4. W ofercie muszą zostać jednoznacznie wskazane (np. poprzez podanie kodu produktu) oba komponenty/produkty.
15. Zamawiający dedykuje dla celu instalacji komponentu zarządczego następujące zasoby serwerowe:
	* 1. 16 vCPU;
		2. 64GB pamięci RAM;
		3. 1TB przestrzeni dyskowej (bez uwzględnienia przestrzeni na logi).

**VIII. WYMAGANIA LICENCYJNE ORAZ AKTYWNEGO WSPARCIA TECHNICZNEGO**

1. Całość rozwiązania musi pochodzić od jednego producenta.
2. Aktywne wsparcie techniczne obejmować będzie co najmniej poziom:
	1. Zapewnienie kompleksowego i wielopoziomowe wsparcie techniczne oraz doradcze dla oferowanych produktów poprzez oddelegowanie dedykowanego zespołu doświadczonych inżynierów produktu dostępnych 24 godziny na dobę, 7 dni w tygodniu, z czasem reakcji na poziomie do dwóch godzin roboczych.
	2. Wszystkie zgłoszenia problemów oraz awarii otrzymają najwyższy możliwy priorytet żądań, aby zapewnić jak najszybsze rozwiązanie problemu. Dopuszczalne jest wsparcie zarówno realizowane przez producenta jak i wskazanego autoryzowanego partnera.
	3. W przypadku zaistnienia awarii sprzętowej urządzenia, zostanie ono wymienione na urządzenie pozbawione wad w ciągu następnego dnia roboczego (tryb NBD).
	4. Wsparcie obejmować będzie okres co najmniej **60 miesięcy**.
3. W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres **60 miesięcy**.
4. Dla systemu firewall należy dostarczyć usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla następujących funkcji:
	1. Aktualizacje bazy aplikacji;
	2. Aktualizacje baz sygnatur IPS;
	3. Aktualizacje baz sygnatur AV;
	4. Dostęp do bazy URL zapewniającej informacje o kategoryzacji strony i powiązanym z nią poziomie ryzyka
	5. Możliwość współpracy z systemem sandbox
	6. Aktualizacji baz dla ochrony DNS;
	7. Realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN).

**IX. WDROŻENIE I SZKOLENIA**

W ramach realizacji zamówienia Wykonawca przeprowadzić ma wdrożenie dostarczonych rozwiązań sprzętowo-programowych. Wdrożenie poprzedzone musi zostać analizą przedwdrożeniową przeprowadzoną wspólnie z Zamawiającym. Wdrożenie musi przebiegać w sposób jak najmniej przerywającym codzienną pracę systemów informatycznych Zamawiającego. W ramach analizy przedwdrożeniowej należy uwzględnić analizę obecnych ustawień, konfiguracji i polityk obecnego rozwiązania systemu firewall. Należy zaplanować nowe rodzaje polityk, harmonogram wdrożenia i przełączeń, ewentualne plany awaryjne oraz naprawcze w trakcie realizacji prac rekonfiguracyjnych i połączeniowych. Po etapie wdrożenia Wykonawca zobowiązany jest do przedstawienia Zamawiającemu dokumentacji powykonawczej wdrożonego rozwiązania, której zakres zostanie opracowany na etapie analizy przedwdrożeniowej.

W ramach postępowania należy dostarczyć vouchery na szkolenia autoryzowane przez producenta oferowanego rozwiązania. Vouchery muszą być ważne przez okres 6 miesięcy.

Zakres szkoleń:

1. Szkolenie dotyczące konfiguracji i zarządzania dla oferowanych rozwiązań, pozwalające uczestnikom biorącym udział w tym szkolenie na zdobycie praktycznej wiedzy z zakresu konfiguracji systemu operacyjnego zarządzającego urządzeniami zaproponowanymi w rozwiązaniu. Po ukończeniu szkolenia, uczestnicy powinni umieć samodzielnie przygotować nowe urządzenia do pracy oraz jak monitorować pracujące urządzenia. Zostaną na szkoleniu omówione mechanizmy tworzenia polityk bezpieczeństwa oraz dodatkowych funkcji bezpieczeństwa dostępnych na urządzeniach. Tematyka ma obejmować m.in.:
	1. Zapoznanie się z architekturą rozwiązania
	2. Czynności administracyjne związane z zarządzaniem dostępami
	3. Konfiguracja interfejsów i parametrów sieciowych
	4. Konfiguracja polityk bezpieczeństwa
	5. Konfiguracja pod kątem ochrony AV, IPS URL filtering itp.
	6. Konfiguracja deszyfracji
	7. Konfiguracja high availability
	8. Konfiguracja zdalnych połączeń połączeń VPN
	9. Monitorowanie oraz tworzenie raportów
	10. Najlepsze praktyki konfiguracyjne

Dodatkowe wymagania:

* + 1. Czas trwania kursu: do 5 dni
		2. Ilość osób uczestniczących w szkoleniu: 4 osoby
1. Zaawansowane szkolenie związane z rozwiązywaniem problemów dotyczących oferowanych rozwiązań w zakresie obejmującym co najmniej poszerzenia wiedzy o umiejętności wyszukiwania oraz diagnozowanie problemów w zaoferowanych urządzeniach. Szkolenie wykorzystujące możliwość dostępu do wirtualnego laboratorium, w którym odwzorowane zostaną rzeczywiste problemy związane z pracą urządzenia w takich aspektach oraz funkcjach systemu operacyjnego urządzenia jak bezpieczeństwo, sieć, ochrona przed zagrożeniami, logowanie, raportowanie, wydajność. Po zakończeniu szkolenia uczestnicy będą posiadać głęboką wiedzę na temat rozwiązywania problemów z widocznością i kontrolą aplikacji, użytkowników oraz zawartości. Tematyka ma obejmować m.in.:
	1. Logika przepływu ruchu
	2. Rozwiązywanie problemów z deszyfracją
	3. Packet capture
	4. Rozwiązywanie problemów związanych ze zdalnymi połączeniami VPN
	5. Rozwiązywanie problemów związanych z zagadnieniami typu identyfikacja użytkowników, identyfikacja aplikacji itp.
	6. Usługi systemowe

Dodatkowe informacje

* 1. Czas trwania kursu: do 3 dni
	2. Ilość osób uczestniczących w szkoleniu: 1 osoba