[1. NIETECHNICZNE CECHY URZĄDZEŃ 2](#_Toc170907624)

[2. DODATKOWE SYSTEMY ZEWNĘTRZNE 3](#_Toc170907625)

[3. WYMAGANIA OGÓLNE DLA NGFW – 2 szt. 4](#_Toc170907626)

[4. WYMAGANIA FUKCJONALNE DLA ROZWIĄZAŃ NGFW 5](#_Toc170907627)

[Cechy NGFW 5](#_Toc170907628)

[Silniki detekcyjne i ochronne NGFW 5](#_Toc170907629)

[Obsługa VPN oraz funkcji sieciowych 7](#_Toc170907630)

[Uwierzytelnienie i ustalanie tożsamości użytkowników 7](#_Toc170907631)

[Zarządzenie urządzeniami NGFW 8](#_Toc170907632)

[Interpretacja parametrów wydajnościowych NGFW 8](#_Toc170907633)

[5. WYMAGANIA LICENCYJNE 9](#_Toc170907634)

[6. WYMAGANIA GWARANCYJNE 9](#_Toc170907635)

[7. KRYTERIA PUNKTOWANE 11](#_Toc170907636)

[Zaawansowana ochrona DNS – 10 PKT 11](#_Toc170907637)

[Ochrona z wykorzystaniem mechanizmów Machine Learning - 10 PKT 11](#_Toc170907638)

# NIETECHNICZNE CECHY URZĄDZEŃ

1. Przedmiot zamówienia musi być legalny, 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 (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. 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.

# 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 i dobrowolne. Decyzja o ich zastosowaniu leży w gestii Wykonawcy – jeżeli uzna on, 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:

1. weryfikacji tożsamości użytkowników – system uwierzytelniania;
2. realizacji funkcji zarządzania firewallem i uprawnieniami administratorów;
3. zatwierdzania zmian w konfiguracji;
4. realizacji funkcji inspekcji ruchu SSL;
5. realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania.

W przypadku stosowania systemów wspomagających Zamawiający wymaga by były one oferowane przez tego samego producenta co oferowany system firewall i całościowo serwisowane przez tego producenta.

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.

# WYMAGANIA OGÓLNE DLA NGFW – 2 szt.

1. **Firewall musi być dostarczone w postaci dedykowanego rozwiązania sprzętowo-programowego – tzw. appliance.**
2. **Cechy wydajnościowe:**
	1. 2,5 Gbps przepustowości Firewall/kontroli aplikacji;
	2. 1 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
	3. 1 Gbps dla IPsec VPN;
	4. 190 000 jednoczesnych sesji;
	5. 32 000 nowych połączeń na sekundę;
	6. 1000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;
	7. 3 wirtualne routery posiadające odrębne tabele routingu;
	8. 50 stref bezpieczeństwa;
	9. Lokalna przestrzeń pamięci co najmniej o pojemności 100GB przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi)
3. **Cechy urządzenia – interfejsy, zasilanie:**
	1. Wysokość maksymalnie 1U;
	2. Urządzenie musi być montowane w szafie RACK 19”, należy dostarczyć stosowne akcesoria.
	3. 8 portów 1-GigabitEthernet RJ45 (dopuszcza się uzyskanie tych portów poprzez zastosowanie portów 1 GigabitEthernet SFP obsadzonych modułami z RJ45)
	4. 1 port 1-GigabitEthernet RJ45 wyłącznie do celów zarządzania (dopuszcza się uzyskanie tego portu poprzez zastosowanie portu SFP obsadzonego modułem RJ45)
	5. Port konsolowy do celów zarządzania

# WYMAGANIA FUKCJONALNE DLA ROZWIĄZAŃ NGFW

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.

## 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 65 535 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. Ochrona DNS,
	5. sandbox lokalny lub chmurowy tego samego producenta
	6. kategoryzacja i filtracja URL
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

## Silniki detekcyjne i ochronne NGFW

1. 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.
2. Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.
3. Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
4. 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 lub 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.
5. Wykrywanie aktywności sieci typu Botnet.
6. Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
7. Podstawowa ochrona DNS co najmniej w zakresie:
	1. wykrywanie zapytań do domen złośliwych.
	2. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
8. 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.
9. Funkcja ochrony przed zagrożeniami Day0 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)
	2. możliwość aktualizacji systemu firewall o nowo wykryte (w Sandbox) zagrożenia.
	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. Możliwość jednoczesnej analizy minimum 24 próbek (VM Sandboxing). Dopuszcza się realizację funkcji sandbox zarówno w chmurze producenta jak i w poprzez lokalne urządzenia sandbox.
	5. Jednoczesna analiza 24 próbek/plików musi być zapewniona bez względu na to czy pliki te będą wysyłane automatycznie czy manualnie przez administratora czy też będzie to „mix” plików pochodząca zarówno bezpośrednio z firewalla jak też od administratorów.
10. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).
11. Rozwiązanie musi posiadać funkcjonalność deszyfracji połączeń SSL/TLS.

## 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.
	1. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW- obsługa co najmniej 1000 tuneli/użytkowników.
	2. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS, Android, iOS
	3. Oprogramowanie klienta VPN musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji zdalnej Windows i MACOS co najmniej w zakresie sprawdzenia:
		1. czy zainstalowano oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury
		2. czy włączony jest osobisty firewall
		3. czy komputer jest komputerem w domenie Active Directory (tylko Windows)
	4. Rozwiązanie musi zapewniać dostęp z wykorzystaniem przeglądarki internetowej bez konieczności instalacji klienta (ang. clientless access)
	5. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewalla.
	6. Jeżeli oprogramowanie klienta jest dodatkowo licencjonowane przez producenta wówczas należy przewidzieć je dla 1500 użytkowników/urządzeń oraz zapewnić możliwość licencyjnej rozbudowy do 2000.
3. Obsługa protokołów routingu: OSPFv2 i OSPFv3, BGP4;
4. Obsługa 4094 VLAN zgodnych z 802.1q.
5. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
6. 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.
7. 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.
8. 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.

## Uwierzytelnienie i ustalanie tożsamości użytkowników

1. 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;
2. 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.
3. Uwierzytelnianie administratorów NGFW za pomocą:
	1. bazy lokalnej;
	2. zewnętrznej usługi katalogowej dostępnej po LDAPS;
	3. RADIUS lub TACACS+.

## Zarządzenie urządzeniami NGFW

1. 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.
2. Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
3. 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.

## Interpretacja parametrów wydajnościowych NGFW

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.

# WYMAGANIA LICENCYJNE

1. Całość rozwiązania będzie pochodziła od jednego producenta.
2. W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 60 miesięcy.
3. 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. Możliwość współpracy z systemem sandbox;
	5. Aktualizacji baz dla ochrony DNS;
	6. realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN);

# WYMAGANIA GWARANCYJNE

1. Zamawiający wymaga aby dostarczone urządzenia zostały objęte 60 miesięcznym serwisem gwarancyjnym, opartym na pakietach serwisowych producenta.
2. Zamawiający wymaga aby serwis gwarancyjny zapewniał:
	1. możliwości zgłaszania awarii i usterek w trybie 24x7, przez 7 dni w tygodniu, 365 dni w roku przez cały okres obowiązywania umowy,
	2. czas reakcji liczony od terminu przyjęcia zgłoszenia do 1 godziny,
	3. bezpłatny dostęp do pomocy technicznej, w tym diagnozę oraz zdalną asystę techniczną inżyniera,
	4. w przypadku awarii sprzętowej - wymianę sprzętu w trybie NBD,
	5. dostęp do zasobów producenta: dokumentacji technicznej dot. posiadanych urządzeń, internetowej bazy wiedzy,
	6. dostęp do nowych wersji oprogramowania i aktualizacji,
3. Zamawiający wymaga aby przed podpisaniem protokołu odbioru, Wykonawca dostarczył informacje o serwisie gwarancyjnym – opis usługi, procedurę zgłaszania awarii, dostępne kanały komunikacyjne.
4. Wykonawca zapewni przynajmniej 2 kanały umożliwiające zgłaszanie problemów.

# KRYTERIA PUNKTOWANE

## Zaawansowana ochrona DNS – 10 PKT

Zaawansowana ochrona DNS w trybie rzeczywistym. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej

* + 1. wykrywanie zapytań do domen złośliwych.
		2. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
		3. wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)
		4. wykrywanie domen fast flux
		5. wykrywanie domen dynamicznych Dynamic DNS
		6. wykrywanie domen nowo rejestrowanych – Newly-registered-domain
		7. Wykrywanie domen strategically-aged-domain
		8. wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych
		9. wykrywanie ataków DNS Tunelling
		10. wykrywanie ataków na rekordy DNS
		11. wykrywanie ataków na protokół DNS

Zamawiający przyzna dodatkowe 10 punktów, jeżeli dostarczony system firewall umożliwi realizację funkcji opisanej w p.1. przez okres co najmniej 60 miesięcy.

## Ochrona z wykorzystaniem mechanizmów Machine Learning - 10 PKT

Urządzenie NGFW musi pozwalać na blokowanie zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanego dynamicznie przez producenta. Wykrywanie i blokowanie złośliwych treści musi odbywać się lokalnie na urządzeniu, jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych oraz funkcji filtrowania URL. Funkcja wykrywania zagrożeń z wykorzystaniem mechanizmów ML musi być dostępna co najmniej dla:

* + 1. Złośliwych plików wykonywalnych (PE);
		2. Złośliwych skryptów PowerShell;
		3. złośliwych skryptów JavaScript;
		4. ataków phishing;

Wykonawca, który deklaruje spełnienie kryterium musi oferować urządzenia pozwalające blokowanie zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanego dynamicznie przez producenta. Wykrywanie i blokowanie złośliwych treści musi odbywać się lokalnie na urządzeniu, jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych oraz funkcji filtrowanie URL.

Zamawiający przyzna dodatkowe 10 punktów, jeżeli dostarczony system firewall umożliwi realizację funkcji opisanej w p.2. przez okres co najmniej 60 miesięcy.