# Załącznik Nr 2 do SWZ: Szczegółowy opis przedmiotu zamówienia

# System bezpieczeństwa:

## Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* firewall,
* ochrony w warstwie aplikacji,
* protokołów routingu dynamicznego.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Rzeczpospolitej Polskiej, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Zamawiający wymaga zaoferowania sprzętu z oficjalnego/autoryzowanego kanału sprzedaży producenta z przeznaczeniem na rynek Rzeczypospolitej Polskiej. Oferowane rozwiązanie musi posiadać pełną funkcjonalność, gwarancję oraz wsparcie techniczne w miejscu użytkowania, którym jest siedziba zamawiającego.

## Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

## Interfejsy, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować (nie wliczając w to portów do zarządzania i utworzenia klastra) minimum:
* 6 portami Ethernet 1Gbps (RJ-45/SFP).
* 2 portami Ethernet 10 Gbps (RJ-45/SFP+).
1. System Firewall musi posiadać wbudowany port konsoli szeregowej.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

## Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 35 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 25 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 35 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 15 Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu typu Enterprise Mix - minimum 10 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.

## Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Zarządzanie pasmem (QoS, Traffic shaping).
8. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
9. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Analiza ruchu szyfrowanego protokołem SSL.
11. Analiza ruchu szyfrowanego protokołem SSH.

## Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* translację jeden do jeden oraz jeden do wielu,
* dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu:
* VMware vCenter (ESXi),
* VMware NSX,
* OpenStack.

## Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* wsparcie dla IKE v1 oraz v2,
* obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM),
* obsługa protokołu Diffie-Hellman grup 19 i 20,
* wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,
* tworzenie połączeń typu Site-to-Site oraz Client-to-Site,
* monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
* możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,
* obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,
* mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0,
* pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta,
* producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

## Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
* routingu statycznego,
* Policy Based Routingu,
* protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

## Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

## Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

## Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

## Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

## Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

## Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

## Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

## Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

## Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

## Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

## Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować na okres minimum 36 miesięcy:

* Kontrolę Aplikacji,
* IPS,
* Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
* Analizę typu Sandbox,
* Web Filtering,
* bazy reputacyjne adresów IP/domen.

## Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# System ochrony poczty

## Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Rzeczpospolitej Polskiej, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Zamawiający wymaga zaoferowania sprzętu z oficjalnego/autoryzowanego kanału sprzedaży producenta z przeznaczeniem na rynek Rzeczypospolitej Polskiej. Oferowane rozwiązanie musi posiadać pełną funkcjonalność, gwarancję oraz wsparcie techniczne w miejscu użytkowania, którym jest siedziba zamawiającego.

## Parametry fizyczne systemu antyspamowego

1. System musi być wyposażony w minimum 2 porty Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB.
3. System musi posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

## Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

System musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2, oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

## Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 100 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 150 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention).
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
19. Możliwość integracji z Office 365 oraz serwerami Exchange z wykorzystaniem API.

## Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu virus-outbreak.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

## Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antyspamowej.
13. Ochrona typu outbreak.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

## Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

## Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

## Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe mozliwości:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

## Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz URL uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

## Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

## Certyfikaty

1. VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.

## Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować na okres minimum 36 miesięcy:

* kontrolę Antyspam,
* URL Filtering,
* kontrolę antywirusową,
* ochrona typu Virus Outbreak,
* sandbox w chmurze,
* ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise.

## Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Centralny system logowania, raportowania i korelacji

## Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 6.5, 6.7; Microsoft Hyper-V wersje: 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Rzeczpospolitej Polskiej, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Zamawiający wymaga zaoferowania produktu z oficjalnego/autoryzowanego kanału sprzedaży producenta z przeznaczeniem na rynek Rzeczypospolitej Polskiej. Oferowane rozwiązanie musi posiadać pełną funkcjonalność, gwarancję oraz wsparcie techniczne w miejscu użytkowania, którym jest siedziba zamawiającego.

## Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

## Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 25 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

## Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
* listę najczęściej wykrywanych ataków,
* listę najbardziej aktywnych użytkowników,
* listę najczęściej wykorzystywanych aplikacji,
* listę najczęściej odwiedzanych stron www,
* listę krajów , do których nawiązywane są połączenia,
* listę najczęściej wykorzystywanych polityk Firewall,
* informacje o realizowanych połączeniach IPSec.
1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

## Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

## Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* malware,
* aplikacje sieciowe,
* email,
* IPS,
* traffic,
* systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

## Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

## Gwarancja oraz wsparcie

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. System musi być objęty serwisem producenta przez okres minimum 36 miesięcy, upoważniającym do aktualizacji oprogramowania i do codziennej aktualizacji bazy skompromitowanych hostów w oparciu o adresy IP, domeny i adres URL oraz wsparcia technicznego w trybie 24x7.

# Wdrożenie

## Wdrożenie systemu bezpieczeństwa

* zebranie informacji na temat potrzeb konfiguracyjnych u Zamawiającego
* wstępna konfiguracja urządzenia
* montaż urządzeń na miejscu u Zamawiającego
* konfiguracja urządzenia zgodnie z potrzebami Zamawiającego
* konfiguracja interfejsów i routingów
* konfiguracja klastra wysokiej dostępności HA
* stworzenie profili bezpieczeństwa warstwy siódmej
* konfiguracja polityk zgodnie z wytycznymi Zamawiającego
* konfiguracja zdalnego dostępu SSL VPN
* wykonanie przełączenia produkcyjnego w oknie serwisowym wskazanym przez Zamawiającego
* asysta po wykonaniu przełączenia

## Wdrożenie system ochrony poczty

* zebranie informacji na temat potrzeb konfiguracyjnych u Zamawiającego
* wstępna konfiguracja urządzenia
* montaż urządzeń na miejscu u Zamawiającego
* konfiguracja urządzenia zgodnie z potrzebami Zamawiającego
* konfiguracja interfejsów i routingów
* konfiguracja profili bezpieczeństwa chroniących wskazany serwer poczty elektronicznej
* wykonanie przełączenia produkcyjnego w oknie serwisowym wskazanym przez Zamawiającego
* asysta po wykonaniu przełączenia

## Wdrożenie centralnego systemu logowania, raportowania i korelacji

* instalacja systemu w środowisku wirtualnym u Zamawiającego
* wstępna konfiguracja systemu (Adresacja interfejsów, routingów)
* konfiguracja ilości logów przechowywanych do analizy i archiwizowanych
* konfiguracja urządzeń sieciowych logujących do systemu
* weryfikacja poprawności spływających logów
* wykonanie kilku testowych raportów w celu weryfikacji czy dane są poprawnie zapisywane.

# Szkolenia

## Szkolenia certyfikowane

1. Minimum 3 dniowe szkolenie autoryzowane przez producenta oferowanego NGFW dla 1 osoby obejmujące:
* Wprowadzenie i podstawowa konfiguracja
* Polityki zapory sieciowej
* Translacja adresów sieciowych (NAT)
* Uwierzytelnianie użytkowników
* Logowanie i monitoring
* Operacje oparte na certyfikatach
* Filtr stron www
* Kontrola aplikacji
* Antywirus
* System ochrony przed włamaniami i atakami DoS
* SSL VPN
* Konfiguracja HA
1. Minimum 3 dniowe szkolenie autoryzowane przez producenta oferowanego systemu ochrony poczty elektronicznej dla 1 osoby obejmujące:
* Poczta elektroniczna – przegląd pojęć, protokołów, standardów
* Podstawowa konﬁguracja urządzenia
* Konﬁguracja parametrów serwera poczty elektronicznej
* Kontrola i inspekcja ruchu pocztowego
* Moduł Antispam
* Monitorowanie sesji
* Skanowanie treści oraz archiwizacja
* Uwierzytelnienie i zabezpieczenie komunikacji
* LDAP
* Diagnostyka i rozwiązywanie problemów
* Tryb transparentny
* Konfiguracja HA
* Tryb serwera
1. Minimum 2 dniowe szkolenie autoryzowane przez producenta oferowanego systemu logowania i analizy dla 1 osoby obejmujące:
* Wprowadzenie i wstępna konﬁguracja
* Administracja i zarządzanie
* Rejestracja urządzeń
* Logi i archiwa
* Obsługa incydentów i zdarzeń
* Scenariusze obsługi incydentów i zdarzeń (playbooks)
* Raporty
1. Uczestnicy każdego szkolenia otrzymują certyﬁkat ukończenia szkolenia sygnowany przez autoryzowanego partnera producenta oferowanego rozwiązania.
2. Dopuszcza się szkolenia w formie klasy wirtualnej.

## Szkolenia wprowadzające (niecertyfikowane)

1. Szkolenie wprowadzające prowadzone przez dostawcę oferowanego NGFW obejmujące:
* Wprowadzenie i podstawowa konfiguracja
* Polityki zapory sieciowej
* Translacja adresów sieciowych (NAT)
* Uwierzytelnianie użytkowników
* Logowanie i monitoring
* Operacje oparte na certyfikatach
* Filtr stron www
* Kontrola aplikacji
* Antywirus
* System ochrony przed włamaniami i atakami DoS
* SSL VPN
* Konfiguracja HA
1. Szkolenie wprowadzające prowadzone przez dostawcę oferowanego systemu ochrony poczty elektronicznej obejmujące:
* Poczta elektroniczna – przegląd pojęć, protokołów, standardów
* Podstawowa konﬁguracja urządzenia
* Konﬁguracja parametrów serwera poczty elektronicznej
* Kontrola i inspekcja ruchu pocztowego
* Moduł Antispam
* Monitorowanie sesji
* Skanowanie treści oraz archiwizacja
* Uwierzytelnienie i zabezpieczenie komunikacji
* LDAP
* Diagnostyka i rozwiązywanie problemów
* Tryb transparentny
* Konfiguracja HA
* Tryb serwera
1. Szkolenie wprowadzające prowadzone przez dostawcę oferowanego systemu logowania i analizy obejmujące:
* Wprowadzenie i wstępna konﬁguracja
* Administracja i zarządzanie
* Rejestracja urządzeń
* Logi i archiwa
* Obsługa incydentów i zdarzeń
* Scenariusze obsługi incydentów i zdarzeń (playbooks)
* Raporty

# Audyt bezpieczeństwa

Wykonawca zobowiązany będzie w szczególności do:

* doradzania Zamawiającemu w zakresie wymaganej dokumentacji wynikającej z Zarządzenia nr 68/2022/BBIICD z dnia 20 maja 2022 r. Prezesa NFZ w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów informatycznych świadczeniodawców,
* analizy złożonej Ankiety weryfikacji dojrzałości pod kątem cyberbezpieczeństwa w stosunku do zapotrzebowania i możliwości refinansowania przez NFZ),
* wykonania audytu wstępnego w celu oceny poziomu bezpieczeństwa systemów teleinformatycznych,
* wykonania audytu bezpieczeństwa oceniającego efekty wdrożenia rozwiązań w zakresie cyberbezpieczeństwa.

Celem audytu ma być wykazanie podniesienia poziomu bezpieczeństwa informatycznego w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa. Audyt bezpieczeństwa ma być przeprowadzony zgodnie z wymaganiami określonymi w Załączniku nr 2 do Umowy będącej Załącznikiem nr 2 do Zarządzenia nr 68/2022/BBIICD Prezesa NFZ.

Treść załącznika nr 2 do Zarządzenia nr 68/2022/BBIICD Prezesa NFZ poniżej:

„Wymagania dotyczące audytu bezpieczeństwa

Audyt bezpieczeństwa, o którym mowa w niniejszego zarządzenia może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5),w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1. Certified Internal Auditor (CIA);

1) Certified Information System Auditor (CISA);

2) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

3) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

4) Certified Information Security Manager (CISM);

5) Certified in Risk and Information Systems Control (CRISC);

6) Certified in the Governance of Enterprise IT (CGEIT);

7) Certified Information Systems Security Professional (CISSP);

8) Systems Security Certified Practitioner (SSCP);

9) Certified Reliability Professional;

10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z niniejszym zarządzeniem oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.”

 *(data i podpis uprawnionego przedstawiciela(i) Wykonawcy)*