UMOWA NR /GDOŚ /2020

W dniu …….. w Warszawie pomiędzy:

Skarbem Państwa – Generalną Dyrekcją Ochrony Środowiska z siedzibą w Warszawie, ul. Wawelska 52/54, 00-922 Warszawa, NIP: 7010151052, REGON: 141628410, reprezentowanym przez **Panią Agnieszką Chilmon – Dyrektora Generalnego Generalnej Dyrekcji Ochrony Środowiska**,

zwanym w dalszej części umowy „**Zamawiającym**”,

a

……
……

zwaną/ym dalej „**Wykonawcą**”,

łącznie zwani dalej „**Stronami**”, a każdy z nich z osobna zwany również „**Stroną**”,

została zawarta umowa następującej treści (zwana dalej: „**Umową**”):

§ 1.
Przedmiot Umowy

1. Zamawiający zleca, a Wykonawca zobowiązuje się do spełnienia następujących świadczeń, zwanych dalej „**Przedmiotem Umowy**”:
   1) dostawy nowych urządzeń brzegowych dla Generalnej Dyrekcji Ochrony Środowiska oraz dla Regionalnych Dyrekcji Ochrony Środowiska, zwanych dalej „**nowymi Urządzeniami**”, ich zainstalowania, skonfigurowania i uruchomienia oraz zapewnienia oprogramowania do tych Urządzeń, zwanego dalej „**Oprogramowaniem**”;
   2) odnowienia oraz zakupu na rzecz Wykonawcy usługi wsparcia technicznego i serwisów bezpieczeństwa (supportu), zwanego dalej „**Wsparciem**”, odpowiednio: dla nowych Urządzeń oraz dla dotychczasowych urządzeń brzegowych Generalnej Dyrekcji Ochrony Środowiska oraz Regionalnych Dyrekcji Ochrony Środowiska, zwanych dalej „**dotychczasowymi Urządzeniami**”;
   3) przeprowadzenia dwóch jednodniowych szkoleń, zwanych dalej „**Szkoleniami**”, oddzielnie: dla nowych Urządzeń oraz dla dotychczasowych Urządzeń – w formie rejestrowanego webinarium, dla administratorów urządzeń Fortigate wskazanych przez Zamawiającego, a następnie udostępnienia webinarium Zamawiającemu i tym osobom.
2. W **załączniku nr 1 do Umowy** zostały wymienione Urządzenia i Oprogramowanie, których dotyczy Przedmiot Umowy. **Załącznik nr 2 do Umowy** zawiera opis funkcjonalności Urządzeń i Oprogramowania.
3. Wykonawca wykona Umowę zgodnie z ofertą z dnia……..…….. Kopia formularza ofertowego stanowi **załącznik nr 3 do Umowy**.

4. Dostarczone przez Wykonawcę nowe Urządzenia z chwilą ich odebrania przez Zamawiającego staną się własnością Zamawiającego. Z tą samą chwilą przejdą na Zamawiającego uprawnienia do bezterminowego korzystania z Oprogramowania.
5. W ramach realizacji Przedmiotu Umowy Wykonawca dokona zmigrowania konfiguracji z dotychczasowych Urządzeń na nowe Urządzenia.

§ 2.
Oświadczenia i zobowiązania

1. Wykonawca oświadcza, że posiada niezbędne kwalifikacje i dysponuje wykwalifikowanym personelem oraz narzędziami wymaganymi do należytej realizacji Umowy.
2. Wykonawca oświadcza, że przy wykonywaniu Umowy będzie kierował się dostępną wiedzą, etyką zawodową, obowiązującymi przepisami oraz, że zrealizuje Przedmiot Umowy zgodnie z należytą starannością, właściwą dla podmiotów zajmujących się profesjonalnie realizacją dostaw i świadczeniem usług określonych w § 1.
3. Wykonawca może powierzyć wykonanie części Przedmiotu Umowy innemu podmiotowi (dalej: „**Podwykonawcy**").
4. Wykonawca jest odpowiedzialny wobec Zamawiającego za działania lub zaniechania wszystkich osób zatrudnionych przez siebie do wykonywania Przedmiotu Umowy, a także za działania lub zaniechania Podwykonawców, jak za działania lub zaniechania własne.
5. Opóźnienie w wykonaniu Przedmiotu Umowy lub jego części przez Podwykonawców nie zwalnia Wykonawcy z odpowiedzialności za naruszenie terminów przewidzianych Umową.

§ 3
Termin realizacji Przedmiotu Umowy

1. **Wykonawca do …….. 2020 r. dostarczy do siedziby Zamawiającego i zainstaluje oraz skonfiguruje nowe Urządzenia oraz dostarczy Oprogramowanie do nowych Urządzeń**. Wykonawca powiadomi Zamawiającego drogą elektroniczną, na adres osób do kontaktu, o których mowa w § 10 ust. 1 pkt 1, o planowanym terminie wykonania tych świadczeń z co najmniej 3-dniowym wyprzedzeniem. Zamawiający, w terminie 1 dnia roboczego, może nie wyrazić zgody na ten termin i wyznaczy Wykonawcy inny, późniejszy termin – nie późniejszy jednak niż 5 dni roboczych od daty zaproponowanej przez Wykonawcę. Informacja o innym terminie zostanie przekazana przez Zamawiającego drogą elektroniczną, na adres osoby do kontaktu, o której mowa w § 10 ust. 1 pkt 2. Dostarczenie nowych Urządzeń powinno zostać zrealizowane w dniu roboczym.
2. Wykonawca dostarczy licencje elektroniczne (kody) dotyczące Oprogramowania oraz umożliwiające uruchomienie Wsparcia na adres mailowy Zamawiającego (admin@gdos.gov.pl). Przekazanie tych licencji Zamawiającemu jest warunkiem podpisania Protokołu Odbioru Urządzeń i Oprogramowania, o którym mowa w § 5 ust. 1 pkt 1.
3. Wykonawca gwarantuje, że **usługa Wsparcia będzie świadczona nieprzerwanie przez okres 36 miesięcy** liczonych od dnia podpisania Protokołu Odbioru Urządzeń i Oprogramowania.

4. **Wykonawca przeprowadzi Szkolenia** oraz **udostępni Zamawiającemu webinarium z tych Szkoleń w terminie do .....,** przy czym dokładny termin Szkoleń zostanie ustalony przez Strony zgodnie z procedurą opisaną w § 4 ust. 4. Oba Szkolenia powinny odbyć się w dniach roboczych.

§ 4.
Wykonanie Umowy

1. Nowe Urządzenia wraz z Oprogramowaniem zostaną dostarczone Zamawiającemu na koszt i ryzyko Wykonawcy.
2. Korzyści i ciężary związane z nowymi Urządzeniami i Oprogramowaniem oraz niebezpieczeństwo ich przypadkowej utraty lub uszkodzenia przechodzą z Wykonawcy na Zamawiającego z chwilą dokonania odbioru nowych Urządzeń i Oprogramowania, potwierdzonego podpisanym przez Strony Protokołem Odbioru Urządzeń i Oprogramowania, o którym mowa w § 5 ust. 1 pkt 1, bez uwag i zastrzeżeń. Wykonawca ponosi odpowiedzialność za szkody w majątku Zamawiającego i osób trzecich wyrządzone w związku z realizacją Przedmiotu Umowy, w szczególności w związku z dostarczeniem i wymianą Urządzeń.
3. Wykonawca zobowiązuje się do dostarczenia, zainstalowania i uruchomienia nowych Urządzeń, w siedzibie Zamawiającego, w miejscu wskazanym przez Zamawiającego, w terminie określonym zgodnie z § 3 ust. 1.
4. Wykonawca zobowiązuje się do przeprowadzenia Szkoleń w dniach ustalonych z Zamawiającym, jednak nie wcześniej niż po dokonaniu odbioru, o którym mowa w § 5 ust. 1 pkt 1. Wykonawca wyśle Zamawiającemu, drogą elektroniczną, na adres osób do kontaktu, o których mowa w § 10 ust. 1 pkt 1, propozycję terminu danego Szkolenia na co najmniej 5 dni roboczych przed jego zaproponowanym terminem. Zamawiający w terminie 1 dnia roboczego od otrzymania propozycji, drogą elektroniczną, na adres osoby do kontaktu, o której mowa w § 10 ust. 1 pkt 2, wyrazi zgodę na zaproponowany przez Wykonawcę termin lub zaproponuje inny termin Szkolenia, nie wcześniejszy niż 5 dni po dniu, w którym wysłał swoją propozycję. Jeżeli Wykonawcy ten termin nie będzie odpowiadał, Strony będą ustalać termin szkolenia zgodnie z procedurą opisaną w poprzednich zdaniach.

§ 5.
Odbiory

1. Strony ustalają następujące rodzaje odbiorów:
   1) odbiór nowych Urządzeń i Oprogramowania – wzór Protokołu Odbioru Urządzeń i Oprogramowania jest określony w **załączniku nr 4 do Umowy**;
   2) odbiór całego Przedmiotu Umowy – wzór Protokołu Odbioru Końcowego jest określony w **załączniku nr 5 do Umowy**.
2. Odbiór nowych Urządzeń i Oprogramowania ma na celu potwierdzenie dostarczenia, zainstalowania i uruchomienia zgodnie z Umową nowych Urządzeń, dostarczenia, wdrożenia i skonfigurowania Oprogramowania oraz przekazania licencji, o których mowa w § 3 ust. 2. Zostanie on dokonany najpóźniej następnego dnia roboczego po dostarczeniu nowych Urządzeń i Oprogramowania przez Wykonawcę.

3. W ramach odbioru nowych Urządzeń i Oprogramowania, Zamawiający zastrzega sobie prawo weryfikacji Oprogramowania i wszystkich elementów z nim związanych, takich jak certyfikaty/etykiety producenta Oprogramowania, a także zgodności z Umową licencji, o których mowa w § 3 ust. 2.
4. Do Protokołu Odbioru Urządzeń i Oprogramowania Wykonawca dołączy sporządzoną w języku polskim kartę gwarancyjną producenta tych Urządzeń lub dokument potwierdzający wykupienie od producenta Urządzeń lub autoryzowanego partnera serwisowego gwarancji na takich warunkach. W przypadku braku takiej karty Zamawiający może odmówić dokonania odbioru nowych Urządzeń i Oprogramowania.
5. W przypadku gdy nowe Urządzenia lub Oprogramowanie nie będą zgodne postanowieniami Umowy lub SOPZ, lub nie zostaną odpowiednio zainstalowane lub skonfigurowane, lub licencje, o których mowa w § 3 ust. 2, nie będą odpowiadały warunkom umownym, w szczególności nie będą umożliwiały uruchomienia Wsparcia, Zamawiający odmówi dokonania odbioru, o którym mowa w ust. 1 pkt 1, i podpisania Protokołu Odbioru Urządzeń i Oprogramowania oraz wyznaczy termin, w którym Wykonawca będzie zobowiązany do usunięcia stwierdzonych uchybień. Informację w tym zakresie Zamawiający przekaże Wykonawcy drogą elektroniczną, na adres osoby do kontaktu, o której mowa w § 10 ust. 1 pkt 2. W przypadku, gdy w wyznaczonym przez Zamawiającego terminie Wykonawca nie usunie stwierdzonych uchybień, Zamawiający będzie mógł skorzystać z uprawnień, o których mowa w § 9 ust. 1.
6. Po podpisaniu Protokołu Odbioru Urządzeń i Oprogramowania, przeprowadzeniu i udostępnieniu Zamawiającemu webinarium ze Szkoleń, Zamawiający dokona odbioru Przedmiotu Umowy. Warunkiem podpisania tego Protokołu jest uprzednie przekazanie Zamawiającemu przez Wykonawcę zestawienia dostarczonych Urządzeń, Oprogramowania oraz licencji, o których mowa w § 3 ust. 2. Jeżeli Szkolenia nie zostały przeprowadzone w sposób prawidłowy lub Wykonawca nie udostępnił Zamawiającemu webinarium z tych Szkoleń albo zestawienia, o którym mowa poprzednim zdaniu, Zamawiający odmówi dokonania Odbioru końcowego i wyznaczy Wykonawcy termin na usunięcie zaistniałych uchybień. Po usunięciu uchybień Strony podpiszą Protokół Odbioru Końcowego. W przypadku, gdy w wyznaczonym przez Zamawiającego terminie Wykonawca nie usunie zaistniałych uchybień, Zamawiający będzie mógł skorzystać z uprawnień, o których mowa w § 9 ust. 2.

§ 6.
Gwarancja

1. Wykonawca jest odpowiedzialny względem Zamawiającego za jakość dostarczonych Urządzeń oraz wady zmniejszające ich wartość lub użyteczność, a także za prawidłowe funkcjonowanie Oprogramowania na Urządzeniach.
2. Wykonawca gwarantuje, że dostarczone przez niego Urządzenia będą nieużywane (fabrycznie nowe), a ich funkcjonalność będzie zgodna z wymaganiami opisanymi w załączniku nr 1 i 2 do Umowy, oraz będą posiadać wszelkie niezbędne aprobaty, certyfikaty oraz będą spełniać wymagane normy.
3. Wykonawca gwarantuje, że Oprogramowanie będzie zgodne z wymaganiami opisanymi w Szczegółowych minimalnych parametrach technicznych Sprzętu i Oprogramowania, stanowiącego załącznik nr 2 do Umowy oraz będzie posiadać wszelkie niezbędne aprobaty, certyfikaty oraz będzie spełniać wymagane normy. Wykonawca zapewni

możliwość legalnego, nienaruszającego praw osób trzecich, korzystania przez Zamawiającego z Oprogramowania w zakresie niezbędnym do realizacji zadań opisanych w załączniku nr 1 i 2 do Umowy.

4. Wykonawca udziela ….-letniej gwarancji jakości na dostarczone Urządzenia i Oprogramowanie. Okres, o którym mowa w zdaniu poprzednim, liczony jest od dnia podpisania przez Strony Protokołu Odbioru Końcowego.
5. W przypadku stwierdzenia wad, uszkodzeń, awarii lub usterek w Urządzeniach lub Oprogramowaniu, Wykonawca zobowiązuje się do ich usunięcia lub do dostarczenia Zamawiającemu i zainstalowania oraz skonfigurowania nowych Urządzeń wolnych od wad, o parametrach określonych w Umowie, w taki sposób, że nowe Urządzenie będzie miało pełną funkcjonalność. Gwarancji podlegają usterki, wady materiałowe i konstrukcyjne, w tym niespełnianie funkcji użytkowych Urządzeń deklarowanych przez jego producenta lub Wykonawcę lub awarie i błędy w funkcjonowaniu Oprogramowania. Zgłoszenie wady, uszkodzenia, awarii lub usterki w Urządzeniach lub Oprogramowaniu, zwane dalej „**zgłoszeniem**”, powinno zostać dokonane przez Zamawiającego w okresie gwarancji, o którym mowa w ust. 4.
6. Osoby wskazane przez Zamawiającego, o których mowa w § 10 ust. 1 pkt 1, mogą dokonywać zgłoszeń bez ograniczeń czasowych, przez 24 godziny na dobę, 7 dni w tygodniu, telefonicznie, faksem lub drogą elektroniczną na adres, o którym mowa w § 11 ust. 1 pkt 2.
7. Wykonawca, w terminie do 2 godzin roboczych od otrzymania zgłoszenia, potwierdzi jego otrzymanie oraz przekaże informację o planowanym terminie usunięcia zgłoszonej wady, uszkodzenia, awarii lub usterki. Usunięcie zgłoszonej wady, uszkodzenia, awarii lub usterki powinno nastąpić w ciągu 8 godzin roboczych od otrzymania zgłoszenia. W przypadku bezskutecznego upływu terminu, o którym mowa w poprzednim zdaniu, Zamawiający może skorzystać z uprawnień, o których mowa w § 9 ust. 3.
8. W przypadku, w którym usunięcie zgłoszonej wady, uszkodzenia, awarii lub usterki w Urządzeniach będzie wymagało wymiany elementów lub części zamiennych Urządzeń, Wykonawca zobowiązany jest do zainstalowania odpowiednio elementów lub części zamiennych oryginalnych, fabrycznie nowych.
9. Wykonawca dokona naprawy Urządzeń na własny koszt w miejscu jego instalacji.
10. W przypadku niemożności naprawienia i konieczności wymiany Urządzeń lub uszkodzonych trwałych nośników danych na nowe, uszkodzone trwałe nośniki danych, pozostaną do wyłącznej dyspozycji Zamawiającego.
11. Okres obowiązywania gwarancji będzie automatycznie wydłużany o czas naprawy. W przypadku wymiany elementu na nowy, okres gwarancji dla tego elementu biegnie na nowo od chwili dokonania wymiany elementu.

§ 7.
Wynagrodzenie

1. Za realizację Przedmiotu Umowy Wykonawcy przysługuje wynagrodzenie w kwocie **…… złotych brutto** (słownie: ……. zł brutto), zwane dalej „**Wynagrodzeniem**”. Powyższa kwota uwzględnienia wszelkie koszty związane z realizacją Umowy, niezbędne do jej wykonania, w tym wszystkie opłaty i podatki, w szczególności podatek VAT.

2. Wynagrodzenie będzie płatne na podstawie prawidłowo wystawionej i doręczonej Zamawiającemu przez Wykonawcę faktury VAT. Warunkiem wystawienia faktury VAT przez Wykonawcę jest podpisanie przez Strony Protokołu Odbioru końcowego.
3. Zamawiający dopuszcza złożenie faktury VAT w formie:
   1) papierowej (oryginału) na adres Generalna Dyrekcja Ochrony Środowiska, ul. Wawelska 52/54, 00-922 Warszawa, NIP:7010151052, REGON: 141628410 (zmiana adresu nie wymaga zawierania aneksu do Umowy, lecz jedynie poinformowania Wykonawcy drogą elektroniczną, na adres, o którym mowa w § 11 ust. 1 pkt 2, o nowym adresie Zamawiającego);
   2) ustrukturyzowanego dokumentu elektronicznego, złożonego za pośrednictwem Platformy Elektronicznego Fakturowania, zwanej dalej „**PEF**", zgodnie z ustawą *o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym z dnia 9 listopada 2018 r.* (Dz. U. z 2018 r. poz. 2191).
4. Zamawiający nie dopuszcza przesyłania innych ustrukturyzowanych dokumentów elektronicznych, za wyjątkiem faktury.
5. Zamawiający zobowiązuje się dokonać zapłaty Wynagrodzenia w terminie do 14 dni od:
   1) dnia złożenia w Kancelarii GDOŚ, oryginału prawidłowo wystawionej faktury VAT;
   2) dnia przesłania ustrukturyzowanej faktury elektronicznej za pośrednictwem PEF.
6. Ustrukturyzowana faktura elektroniczna (w przypadku wyboru tej formy dokumentu) powinna zawierać obligatoryjne elementy określone w przepisach prawa oraz min. dane zawierające:
   1) informacje dotyczące odbiorcy płatności;
   2) wskazanie umowy zamówienia publicznego, którego dotyczy faktura.
7. Zamawiający informuje, że identyfikatorem PEPPOL/adresem PEF Zamawiającego, który pozwoli na złożenie ustrukturyzowanej faktury elektronicznej jest NIP: 7010151052.
8. Wykonawca powiadomi Zamawiającego o przesłaniu ustrukturyzowanej faktury elektronicznej na PEF w dniu jej przesłania. Powiadomienie o przesłaniu ustrukturyzowanej faktury elektronicznej zostanie przesłane pocztą elektroniczną na adres ……..
9. Strony postanawiają, że jeżeli rachunek bankowy, którym posługuje się Wykonawca nie będzie ujęty w wykazie podatników, o którym stanowi art. 96b ustawy z dnia 11 marca 2004 r. *o podatku od towarów i usług* (Dz. U. z 2020 r. poz. 106, z późn. zm.) – tzw. „*białej liście podatników VAT*", Zamawiający będzie uprawniony do wstrzymania płatności Wynagrodzenia i nie będzie stanowiło to naruszenia Umowy, a Wykonawca nie będzie w takiej sytuacji domagał się od Zamawiającego odsetek za opóźnienie w zapłacie.
10. Za datę dokonania zapłaty Wynagrodzenia Strony uznają datę obciążenia rachunku Zamawiającego.
11. Wykonawca nie może dokonać przeniesienia swoich wierzytelności przysługujących mu wobec Zamawiającego na osoby lub podmioty trzecie bez uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej.

§ 8.
Prawa własności intelektualnej

1. Wykonawca zapewnia Zamawiającego, że posiada licencje do Oprogramowania w zakresie niezbędnym do wykonania Umowy.
2. Wykonawca gwarantuje, że korzystanie z Oprogramowania oraz usługi Wsparcia w terminach określonych w Umowie i w zakresie określonym w załącznikach nr 1 i 2 do Umowy nie będzie stanowiło naruszenia praw własności intelektualnej Wykonawcy lub podmiotu trzeciego.
3. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne Oprogramowania i Wsparcia, w szczególności za ewentualne roszczenia osób trzecich, wynikające z naruszenia praw własności intelektualnej, w tym za nieprzestrzeganie przepisów ustawy z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz. U. z 2019 r. poz. 1231, ze zm.), w związku z realizacją przedmiotu Umowy, a także z korzystaniem ze Wsparcia lub Oprogramowania. W razie wystąpienia przez osoby trzecie przeciwko Zamawiającemu z roszczeniami z powodu naruszenia praw własności intelektualnej, Wykonawca podejmie wszelkie kroki niezbędne do obrony przed tymi roszczeniami, a w przypadku, gdy wskutek wystąpienia z takimi roszczeniami Zamawiający będzie musiał zaniechać korzystania z Oprogramowania lub Wsparcia, lub zostanie zobowiązany prawomocnym i ostatecznym wyrokiem sądu do zapłaty odszkodowania lub zadośćuczynienia z jakiegokolwiek tytułu na rzecz osób trzecich, Wykonawca naprawi wszelkie szkody wynikające z roszczeń osób trzecich, w tym zwróci koszty i wydatki poniesione w związku z tymi roszczeniami.

§ 9.
Kary umowne

1. W przypadku, gdy w wyznaczonym przez Zamawiającego terminie, o którym mowa w § 5 ust. 5, Wykonawca nie dostarczy Urządzeń oraz Oprogramowania, lub nie zainstaluje i skonfiguruje Urządzeń lub Oprogramowania zgodnie z wymaganiami określonymi w Umowie, lub licencje, o których mowa w § 3 ust. 2, nie będą odpowiadały warunkom umownym, w szczególności nie będą umożliwiały uruchomienia Wsparcia, Zamawiający będzie uprawniony, według swego wyboru do:
   1) wyznaczenia Wykonawcy dodatkowego terminu na dokonanie tych czynności i żądania od Wykonawcy zapłaty kary umownej w wysokości 0,5% Wynagrodzenia za każdy dzień zwłoki w ich realizacji, począwszy od terminu wskazanego w § 3 ust. 1 zdanie pierwsze (naliczona w ten sposób kara umowna za zwłokę nie przekroczy 10% Wynagrodzenia); po bezskutecznym upływie dodatkowego terminu Zamawiający będzie uprawniony do skorzystania z uprawnień, o których mowa w pkt 2;
   2) odstąpienia od Umowy i żądania od Wykonawcy zapłaty kary umownej w wysokości 20% Wynagrodzenia.
2. W przypadku, gdy w wyznaczonym przez Zamawiającego terminie, o którym mowa w § 5 ust. 6, Wykonawca nie przeprowadzi Szkoleń lub nie udostępni Zamawiającemu webinarium z tych Szkoleń, lub nie dostarczy Zamawiającemu zestawienia dostarczonych Urządzeń, Oprogramowania oraz licencji, o których mowa w § 3 ust. 2, Zamawiający

będzie uprawniony do żądania od Wykonawcy zapłaty kary umownej w wysokości 5% Wynagrodzenia.

3. W przypadku nieusunięcia przez Wykonawcę objętej gwarancją, o której mowa w § 6, zgłoszonej przez Zamawiającego wady, uszkodzenia, awarii lub usterki Zamawiający będzie uprawniony, według swego wyboru do:
   1) wyznaczenia Wykonawcy dodatkowego terminu na realizację tego obowiązku i żądania od Wykonawcy zapłaty kary umownej w wysokości 0,1% Wynagrodzenia za każdą godzinę roboczą zwłoki w jego realizacji, począwszy od upływu terminu wskazanego w § 6 ust. 7 zdanie drugie (naliczona w ten sposób kara umowna za zwłokę w realizacji jednego zgłoszenia nie przekroczy 5% Wynagrodzenia); po bezskutecznym upływie dodatkowego terminu Zamawiający będzie uprawniony do skorzystania z uprawnień, o których mowa w pkt 2;
   2) zlecenia podmiotowi trzeciemu usunięcia zgłoszonej przez Zamawiającego wady, uszkodzenia, awarii lub usterki – Wykonawca wyraża zgodę na obciążenie go przez Zamawiającego kosztami usunięcia tej wady przez podmiot trzeci.
4. W przypadku naruszenia przez Wykonawcę obowiązków dotyczących poufności, o których mowa w § 13, Zamawiający będzie uprawniony do żądania od Wykonawcy zapłaty kary umownej w wysokości 5% Wynagrodzenia za każdy przypadek.
5. W przypadku naruszenia przez Wykonawcę obowiązków Umownych w inny sposób niż wskazany w ust. 1-4, Zamawiający będzie uprawniony do żądania od Wykonawcy zapłaty kary umownej w wysokości 5 000 zł za każdy przypadek.
6. Jeżeli wartość szkody przewyższy wartość zastrzeżonych kar umownych, Zamawiający ma prawo dochodzenia odszkodowania uzupełniającego do pełnej wartości poniesionej szkody.
7. Wykonawca wyraża zgodę na potrącenie kar umownych z Wynagrodzenia.
8. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
9. W przypadku odstąpienia od Umowy przez Zamawiającego, Wykonawca zobowiązuje się do odebrania na własny koszt od Zamawiającego dostarczonych Urządzeń lub Oprogramowania, a Zamawiający nie ponosi odpowiedzialności za dostarczone wcześniej Urządzenia lub Oprogramowanie w czasie gdy znajdowały się u Zamawiającego.

§ 10.
Osoby do kontaktu

1. Strony ustalają, że osobami reprezentującymi Strony w zakresie realizacji Umowy, w tym upoważnionymi do podpisywania w imieniu Stron, które je wskazały, Protokołów Odbioru, o których mowa w § 5 ust. 1, uzgadniania terminów realizacji poszczególnych świadczeń w ramach Przedmiotu Umowy oraz dokonywania i przyjmowania zgłoszeń w ramach gwarancji, o której mowa w § 6, są:
   1) ze strony Zamawiającego:
      a) ……., nr tel.: ……., e-mail: ……,

b) ……., nr tel.: ……., e-mail: ……;

2) ze strony Wykonawcy:

a) ……., nr tel.: ……..., e-mail: ……...,

b) ……., nr tel.: ……..., e-mail: ……....

– przy czym każda z tych osób jest upoważniona do samodzielnego działania w imieniu Strony, która ją wskazała.

2. Wykonawca ma możliwość zmiany osób, o których mowa w ust. 1 pkt 2, gdy jest to uzasadnione obiektywnymi okolicznościami, o czym jest zobowiązany niezwłocznie powiadomić Zamawiającego drogą elektroniczną na adres wskazany w § 11 ust. 1 pkt 1.
3. Na żądanie Zamawiającego przekazane Wykonawcy drogą elektroniczną na adres wskazany w § 11 ust. 1 pkt 2, Wykonawca jest zobowiązany, w terminie nie dłuższym niż 3 dni od dnia otrzymania takiego żądania, dokonać zmiany osób, o których mowa w ust. 1 pkt 2, i powiadomić o tym Zamawiającego drogą elektroniczną na adres wskazany w § 11 ust. 1 pkt 1.
4. W przypadku dokonywania zmiany osób, o których mowa w ust. 1 pkt 2, nowa osoba powinna posiadać kompetencje nie niższe niż osoba wymieniana.
5. Zamawiający może dokonać zmiany osób, o których mowa w ust. 1 pkt 1, w każdym momencie, o czym powiadomi Wykonawcę drogą mailową na adres wskazany w § 11 ust. 1 pkt 2.
6. Zmiana osób, wymienionych w ust. 1, dokonana zgodnie z postanowieniami niniejszego paragrafu, nie wymaga zawierania aneksu do Umowy.

§ 11.
Doręczenia

1. Strony wskazują następujące dane kontaktowe, na które należy kierować korespondencję związaną z zawarciem i realizacją Umowy:
   1) dane Zamawiającego: ul. Wawelska 52/54, 00-922 Warszawa, Generalna Dyrekcja Ochrony Środowiska, Biuro Dyrektora Generalnego, tel.: (22) 36-92-523, fax.: (22) 36-62-524, e-mail: sekretariat.bdg@gdos.gov.pl;
   2) dane Wykonawcy: ……..…, tel.: ……..., fax.: ……..., e-mail: ……..
2. Strony mają obowiązek niezwłocznego informowania się wzajemnie o każdej zmianie swoich danych kontaktowych w formie pisemnej i na adres mailowy drugiej Strony wskazany w ust. 1. Powyższa zmiana nie wymaga zawierania aneksu do Umowy. Korespondencja wysłana na ostatnio podane dane kontaktowe Strony uznawana będzie za skutecznie doręczoną drugiej Stronie.
3. O ile Strony nie postanowią inaczej, z zastrzeżeniem ust. 4, Strony będą doręczać sobie korespondencję dotyczącą zawarcia i realizacji Umowy pocztą kurierską lub listem poleconym, lub pocztą elektroniczną, lub faksem, na ostatnio podane przez Stronę dane kontaktowe.

4. Oświadczenie o wypowiedzeniu lub odstąpieniu od Umowy musi zostać złożone w formie pisemnej pod rygorem nieważności i zostać doręczone drugiej Stronie listem poleconym lub pocztą kurierską, na ostatnio podany przez Stronę adres.
5. Korespondencję wysyłaną pocztą elektroniczną uważa się za doręczoną w momencie jej wysłania – w przypadku korespondencji kierowanej do Zamawiającego – na adres e-mail wskazany w ust. 1 pkt 1, a w przypadku korespondencji kierowanej do Wykonawcy – na adres e-mail wskazany w ust. 1 pkt 2.
6. Listy polecone adresowane na ostatnio podany adres Strony, zwrócone przez pocztę lub firmę kurierską ze względu na niepodjęcie przez adresata w terminie, będą traktowane jako skutecznie doręczone do adresata z upływem czternastego dnia od dnia pierwszej próby doręczenia.

§12.
Siła wyższa

1. Strony nie są odpowiedzialne za naruszenie obowiązków wynikających z Umowy w przypadku, gdy wyłączną przyczyną naruszenia jest działanie Siły wyższej.
2. Przez Siłę wyższą należy rozumieć zdarzenie zewnętrzne, którego Strony nie mogły przewidzieć i któremu nie mogły zapobiec, uniemożliwiające wykonanie Umowy w całości lub części, na stałe lub na pewien czas, któremu Strona nie mogła przeciwdziałać przy zachowaniu należytej staranności i które nie wynikło wskutek błędów lub zaniedbań Strony dotkniętej jej działaniem.
3. Na czas działania Siły wyższej obowiązki Strony, których nie jest ona w stanie wykonać ze względu na działanie tej Siły, ulegają zawieszeniu.
4. W przypadku zaistnienia Siły wyższej Strona, której dotyczy jej działanie, zobowiązana jest niezwłocznie poinformować drugą Stronę na piśmie o wystąpieniu Siły wyższej, ze wskazaniem przewidywanego czasu trwania spowodowanej działaniem tej Siły przeszkody w realizacji obowiązków wynikających z Umowy.

§ 13.
Poufność

1. Umowa jest jawna i podlega udostępnianiu na zasadach określonych w przepisach o dostępie do informacji publicznej.
2. Wykonawca, jego personel zatrudniony przy realizacji Umowy, a także Podwykonawcy, zobowiązani są do utrzymania w tajemnicy i nieujawniania osobom trzecim wszystkich informacji lub dokumentów, w których posiadanie weszli w związku z wykonywaniem Umowy. Dane udostępnione Wykonawcy przez Zamawiającego zostaną wykorzystane jedynie przez niego lub jego personel zatrudniony przy realizacji Umowy lub Podwykonawców do celów realizacji Umowy i nie zostaną ujawnione osobom trzecim, bez zgody Zamawiającego.
3. Wykonawca zobowiązuje się do przestrzegania, przy wykonywaniu Umowy, wszystkich postanowień zawartych w obowiązujących przepisach prawa związanych z ochroną danych, a także z ochroną informacji niejawnych oraz ochroną tajemnicy służbowej.

4. Wykonawca zobowiązuje się zabezpieczyć przed dostępem osób trzecich wszelkie urządzenia oraz dane, informacje i dokumenty, przy pomocy których będzie realizował Umowę.
5. Wykonawca nie może, bez uprzedniej pisemnej zgody Zamawiającego, wykorzystywać, upubliczniać lub udostępniać danych i informacji określonych w ust. 2 w innych celach niż wynikające z Umowy.
6. Postanowienia ust. 2 i 5 nie dotyczą informacji publicznych, informacji powszechnie znanych oraz informacji, których udostępnienie następuje na żądanie organów administracji publicznej, jednostek samorządu terytorialnego, sądów, prokuratury lub instytucji organizacji międzynarodowych, w zakresie w jakim te organy lub instytucje są uprawnione do żądania danych na podstawie odrębnych przepisów.

§ 14.
Zmiany Umowy

1. Z zastrzeżeniem ust. 2 wszelkie zmiany Umowy, z wyłączeniem sytuacji, o których mowa w § 7 ust. 3 pkt 1, § 10 ust. 6, § 11 ust. 2 oraz ust. 3 niniejszego paragrafu, wymagają zachowania formy pisemnej pod rygorem nieważności.
2. Strony dopuszczają możliwość istotnej zmiany postanowień Umowy w przypadku zmiany terminu realizacji Umowy z powodu wystąpienia okoliczności zewnętrznych, których nie można było przewidzieć ani im zapobiec (siła wyższa).
3. Zmiany miejsca, w którym mają zostać zrealizowane świadczenia wskazane w § 1 ust. 1 na inne miejsce na terenie m.s.t. Warszawy jest możliwa w przypadku zmiany siedziby Zamawiającego i nie wymaga zawarcia aneksu do Umowy, lecz jedynie poinformowania Wykonawcy o nowym miejscu realizacji tych świadczeń.

§ 15
Postanowienia końcowe

1. Przez użyty w Umowie termin „**dzień roboczy**” Strony rozumieją dzień od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy. Przez użyty w Umowie termin „**godzina robocza**” Strony rozumieją godziny między 8:00 a 16:00 w dni robocze.
2. W sprawach nieuregulowanych Umową mają zastosowanie przepisy prawa powszechnie obowiązującego ,w tym Kodeksu cywilnego.
3. Wszelkie spory między Stronami wynikające z zawarcia lub realizacji Umowy będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
4. Załącznikami do Umowy, stanowiącymi jej integralną część, są:
    1) załącznik nr 1 – lista Urządzenia lub Oprogramowania, których dotyczy Przedmiot Umowy;
    2) załącznik nr 2 – 2 opis funkcjonalności Urządzeń;
    3) załącznik nr 3 – kopia oferty Wykonawcy;
    4) załącznik nr 4 – wzór Protokołu Odbioru Urządzeń i Oprogramowania;
    5) załącznik nr 5 – wzór Protokołu Odbioru Końcowego.

5. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jednym dla Wykonawcy i dwóch dla Zamawiającego.

ZAMAWIAJĄCY	**WYKONAWCA**
……..……	……..……..

Załącznik nr 1 do umowy - lista urządzeń i oprogramowania, których dotyczy przedmiot umowy

Obecne urządzenia				
lp.	Obecne urządzenie	Serial	Odnowienie lub urządzenie docelowe	Data zakończenia wsparcia
1	FortiAuthenticator VM	FAC-VM0A13000502	odnowienie wsparcia	31.05.2019
2	FortiAnalyzer VM	FAZ-VM0000099633	odnowienie wsparcia	31.05.2019
3	FortiMail 200D	FE200D3A12000007	Wymiana na 200F	31.05.2019
4		FE200D3A12000045	Wymiana na 200F	31.05.2019
5	FortiMail-VM02	FEVM020000013908	odnowienie wsparcia	31.05.2019
6	FortiMail-VM08	FEVM080000078570	odnowienie wsparcia	31.05.2019
7	FortiGate 900D	FG900D3916800920	wymiana na 600E	31.05.2019
8	FortiGate 900D	FG900D3916800958	wymiana na 600E	31.05.2019
9	FortiGate 90D	FGT90D3Z14002856	wymiana na 60F	31.05.2019
10	FortiGate 90D	FGT90D3Z14002867	wymiana na 60F	31.05.2019
11	FortiGate 90D	FGT90D3Z14002878	wymiana na 60F	31.05.2019
12	FortiGate 90D	FGT90D3Z14002884	wymiana na 60F	31.05.2019
13	FortiGate 90D	FGT90D3Z14002910	wymiana na 60F	31.05.2019
14	FortiGate 90D	FGT90D3Z14002913	wymiana na 60F	31.05.2019
15	FortiGate 90D	FGT90D3Z14002924	wymiana na 60F	31.05.2019
16	FortiGate 90D	FGT90D3Z14002928	wymiana na 60F	31.05.2019
17	FortiGate 90D	FGT90D3Z14002937	wymiana na 60F	31.05.2019
18	FortiGate 90D	FGT90D3Z14002943	wymiana na 60F	31.05.2019
19	FortiGate 90D	FGT90D3Z14002947	wymiana na 60F	31.05.2019

20	FortiGate 90D	FGT90D3Z14002984	wymiana na 60F	31.05.2019
21	FortiGate 90D	FGT90D3Z14003038	wymiana na 60F	31.05.2019
22	FortiGate 90D	FGT90D3Z14003291	wymiana na 60F	31.05.2019
23	FortiGate 90D	FGT90D3Z14003294	wymiana na 60F	31.05.2019
24	FortiGate 90D	FGT90D3Z14003295	wymiana na 60F	31.05.2019
25	FortiGate 90D	FGT90D3Z14003310	wymiana na 60F	31.05.2019
26	FortiWeb VM02	-	Nowy zakup	-

Generalna Dyrekcja Ochrony Środowiska obecnie posiada następujące urządzenia, dla których przedmiotem zakupu jest odnowienie wsparcia:
FortiAuthenticator VM FAC-VM0A13000502 - odnowienie wsparcia producenta i dostęp do aktualizacji na 3 lata.
FortiAnalyzer VM FAZ-VM0000099633 - odnowienie wsparcia producenta i dostęp do aktualizacji na 3 lata.
FortiMail-VM02 FEVM020000013908 - odnowienie wsparcia producenta i dostęp do aktualizacji na 3 lata.
FortiMail-VM08 FEVM080000078570 - odnowienie wsparcia producenta i dostęp do aktualizacji na 3 lata.

W ramach wdrożenia Zamawiający pragnie doszczegółowić, że w każdym urządzenia Fortigate należy zmigrować konfigurację z urządzeń obecnych na nowe. Obecne konfiguracje zostaną przesłane do GDOŚ i tutaj zostaną wgrane do nowych urządzeń RDOŚ. Dalszą dystrybucją urządzeń do RDOŚ zajmie się GDOŚ.

Załącznik nr 2 do umowy – ***opis funkcjonalności urządzeń i oprogramowania***

System ochrony poczty elektronicznej 2 sztuki (klaster HA) – FortiMail – 200F-HA

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 lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o 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).

Parametry fizyczne systemu antyspamowego

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

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 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 lub IMAP.
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. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

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 60 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 wirus outbrake.
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 dla 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 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
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 (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie 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 jak również danych historycznych.
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 funkcje:

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.
5. W ramach postępowania wymaganym jest dostarczenie systemu w formie klastra realizującego funkcje podstawowe, gdzie każdy jego element charakteryzuje się parametrami fizycznymi i funkcjonalnymi opisanymi w tym dokumencie.

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

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, 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:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

Gwarancja oraz wsparcie

2. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 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.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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 Polski, 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.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System ochrony aplikacji webowych (WAF) – 1 sztuka – Forti Web VM02

System ochrony aplikacji webowych oraz Firewall XML, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w ww środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny.

Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3. Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4. Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5. Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi obsługiwać minimum:
   - 4 interfejsy sieciowe
   - Ilość wirtualnych procesorów: 2
   - Ilość RAM minimum 24 GB
2. Obsługa powierzchni dyskowej - minimum 1 TB.

Parametry wydajnościowe

1. Przepustowość dla ruchu http - min 100 Mbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Obsługa protokołów: - http 1.1, http 2.0, FTP.
2. Automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu. Możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora.
3. Automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników

4. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
5. Wsparcie dla mechanizmów session persistence:
   - Source IP
   - HTTP Header
   - URL parameter
   - Insert Cookie
   - Rewrite Cookie
   - Persistent Cookie
   - Embedded Cookie
   - ASP Session ID
   - PHP Session ID
   - JSP Session ID
   - SSL Session ID
6. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.
7. Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.
8. Ochrona aplikacji www przed takimi zagrożeniami jak:
   - SQL and OS Command Injection.
   - Cross Site Scripting (XSS).
   - Cross Site Request Forgery.
   - Outbound Data Leakage.
   - HTTP Request Smuggling.
   - Buffer Overflow.
   - Encoding Attacks.
   - Cookie Tampering / Poisoning.
   - Session Hijacking.
   - Broken Access Control.
   - Forceful Browsing /Directory Traversal.
   - Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP.
   - DoS w warstwie aplikacji.
   - Ochrona przed atakami typu Brute force.
   - Ochrona przed atakami clickjacking.
   - Ochrona przed credential stuffing.
9. Mechanizmy ochrony przed wyciekiem informacji poufnych.
10. Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
11. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
12. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.
13. Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.

14. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only”.
15. Content routing na bazie parametrów http oraz certyfikatów X.509.
16. Ochrona przed Web Scraping.
17. Wsparcie dla kompresji danych oraz cache.
18. Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos).
19. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
20. Ochrona przed atakami typu SLOW (Slowloris i podobne).
21. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
    - Metoda HTTP.
    - IP klienta.
    - Host.
    - URI.
    - Cały URL.
    - Parametr.
    - Cookie.
    - http Header
    - JSON Elements
22. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.
23. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
24. Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
25. Ustawienie wymaganej sekwencji otwieranych stron.
26. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML.
27. Wsparcie dla walidacji OpenAPI, JSON i XML.
28. Blokowania „Illegal XML Format” oraz „Illegal JSON Format”.
29. Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.
30. Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
31. Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
32. URL Encryption.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji http realizowana na firewall’u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. 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.
2. Skaner aplikacji WWW realizowany bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć

możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.
3. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.
4. Dekodowanie Base64 oraz CSS.
5. Domyślne szablony ochrony dla Exchange, SharePoint i WordPress.
6. Uwierzytelnianie użytkowników w oparciu o protokół SAML.
7. Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji.
8. Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników.
9. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa.
10. Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day.
11. Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy.
12. Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych.
13. Cross-Origin Resource Sharing (CORS) protection.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.
2. Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

Certyfikaty

1. Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego.

Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
   - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem wsparcia technicznego w trybie 24x7 przez okres 36 miesięcy.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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 Polski, 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.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System do ochrony styku z siecią Internet pełniący również funkcję Data Center Firewall w siedzibie głównej – 2 sztuki klaster HA – FG-600E - HA

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 lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 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.

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. Co najmniej dwa urządzenia dla zbudowania klastra wysokiej dostępności.
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, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w co najmniej dwa redundantne zasilacze 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 36 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 36 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 Enterprise Traffic Mix - minimum 10 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 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, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. 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.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. 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.

- Amazon Web Services (AWS).
- Microsoft Azure
- Cisco ACI.
- Google Cloud Platform (GCP).
- Nuage Networks VSP.
- OpenStack.
- VMware vCenter (ESXi).
- VMware NSX.

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.
2. 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.

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 (np. FTP na porcie 2021).
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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - 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.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. 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) posiadanej przez zamawiającego FortiAnalyzer. Jeśli Oferowane rozwiązanie nie wspiera logowanie do urządzenia FortinAnlayzer zgodnie z poniższymi wymaganiami, należy dostarczyć rozwiązanie które będzie pozwalało na centralne zbieranie logów w ilości 2 GB logów na dzień i pozwalało na przechowanie 1 TB logów. Rozwiązanie może być dostarczone w wersji wirtualnej do uruchomienia na platformie Vmware.
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:

b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 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.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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 Polski, 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.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System do ochrony styku z siecią Internet pełniący również funkcję Data Center Firewall lokalizacjach terenowych – 16 sztuk – FG-60F

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 lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 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.

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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 6 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.

6. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

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, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. 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.
11. Analiza ruchu szyfrowanego protokołem SSL.

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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. 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.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - Nuage Networks VSP.

- OpenStack.
- VMware vCenter (ESXi).
- VMware NSX.

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.
2. 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.

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 (np. FTP na porcie 2021).
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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - 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.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. 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

5. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) posiadanej przez zamawiającego FortiAnalyzer. Jeśli Oferowane rozwiązanie nie wspiera logowanie do urządzenia FortinAnlayzer zgodnie z poniższymi wymaganiami, należy dostarczyć rozwiązanie które będzie pozwalało na centralne zbieranie logów w ilości 2 GB logów na dzień i pozwalało na przechowanie 1 TB logów. Rozwiązanie może być dostarczone w wersji wirtualnej do uruchomienia na platformie Vmware.
6. 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.
7. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
8. 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:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 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.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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 Polski, 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.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Załącznik nr 4 do umowy – ***wzór protokołu odbioru urządzeń i oprogramowania***

PROTOKÓŁ ODBIORU URZĄDZEŃ I OPROGRAMOWANIA

sporządzony w dniu ..... r.

dotyczy: umowy Nr ……...../GDOŚ/2020 zawartej w dniu ..... 2020 r. (zwanej dalej: „Umową")

Wykonawca: .....

1. Zamawiający stwierdza, że w dniu: …… Wykonawca dokonał/nie dokonał[1] dostarczenia, zainstalowania i uruchomienia zgodnie z Umową następujących urządzeń:

lp.	Nazwa Urządzenia	Numer seryjny	Uwagi
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			

[1] Niepotrzebne skreślić. W przypadku niedokonania w stosunku do któregoś urządzenia wymaganych umową czynności wpisać adnotację w uwagach

2. Zamawiający stwierdza, że w dniu: …… Wykonawca dokonał/nie dokonał[2] wdrożenia i skonfigurowania Oprogramowania oraz przekazania licencji, o których mowa w § 3 ust. 2 Umowy

Uwagi[3]:

……
……
……
……
……
……
……

W związku z powyższym **Zamawiający dokonał/nie dokonał[4] odbioru Urządzeń i Oprogramowania**, o którym mowa w § 5 ust. 1 pkt 1 Umowy.

Uwagi[3]:

……
……
……
……
……
……
……

W czynnościach odbioru udział wzięli:

Przedstawiciel Zamawiającego –
.....;

Przedstawiciel Wykonawcy –
.....

Uwagi: .....

Przedstawiciel Zamawiającego **Przedstawiciel Wykonawcy**

....

[2] Niepotrzebne skreślić. Jeżeli Wykonawca nie wykonał którejś z wymaganych umową czynności, wpisać to w uwagach.
[3] W przypadku braku uwag wpisać „Bez uwag".
[4] Niepotrzebne skreślić.

Załącznik nr 5 do umowy – ***wzór protokołu odbioru końcowego***

PROTOKÓŁ ODBIORU KOŃCOWEGO

sporządzony w dniu ..... r.

dotyczy: umowy Nr ……...../GDOŚ/2020 zawartej w dniu ..... 2020 r. (zwanej dalej: „Umową")

Wykonawca: .....

3. Zamawiający stwierdza, że Wykonawca dokonał/nie dokonał[5] dostarczenia, zainstalowania i uruchomienia zgodnie z Umową następujących wszystkich urządzeń wymaganych Umową:

4. Zamawiający stwierdza, że Wykonawca dokonał/nie dokonał[6] wdrożenia i skonfigurowania Oprogramowania oraz przekazania licencji, o których mowa w § 3 ust. 2 Umowy.
5. Zamawiający stwierdza, że Wykonawca w dniach …… przeprowadził Szkolenia, o których mowa w Umowie, oraz udostępnił webinarium ze Szkoleń.
6. Zamawiający stwierdza, że Wykonawca przekazał mu zestawienie dostarczonych Urządzeń, Oprogramowania oraz licencji, o których mowa w § 3 ust. 2 Umowy.

Uwagi[7]:

……
……
……
……
……
……
……

W związku z powyższym Zamawiający dokonał/nie dokonał[8] odbioru końcowego, o którym mowa w § 5 ust. 1 pkt 2 Umowy.

Uwagi[3]:

……
……
……
……
……

[5] Niepotrzebne skreślić. W przypadku niedokonania w stosunku do któregoś urządzenia wymaganych umową czynności wpisać adnotację w uwagach

[6] Niepotrzebne skreślić. Jeżeli Wykonawca nie wykonał którejś z wymaganych umową czynności, wpisać to w uwagach.

[7] W przypadku braku uwag wpisać „Bez uwag".

[8] Niepotrzebne skreślić.

……
……

W czynnościach odbioru udział wzięli:

Przedstawiciel Zamawiającego –
.....;

Przedstawiciel Wykonawcy –
.....

Uwagi: .....

Przedstawiciel Zamawiającego	**Przedstawiciel Wykonawcy**
.....	.....