SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

(zwany dalej: „SOPZ")

Przedmiotem zamówienia jest rozbudowa aktualnie użytkowanego u Zamawiającego systemu ochrony sieci i bezpiecznych tuneli VPN opartego o rozwiązanie firmy Fortinet o kolejne urządzenia sieciowe wraz z wdrożeniem oraz przedłużenie gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego dla systemów bezpieczeństwa teleinformatycznego Generalnej Dyrekcji Ochrony Środowiska.

I. INFORMACJE OGÓLNE DOTYCZĄCE ZAMÓWIENIA

1. Oferowane w ramach Zamówienia produkty muszą spełniać wszystkie parametry określone w SOPZ oraz być fabrycznie nowe, oznakowane symbolem CE tam gdzie jest to wymagane, pochodzić z legalnego źródła, muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęty standardowym pakietem usług gwarancyjnych, zawartych w cenie urządzenia i oprogramowania, świadczonych przez sieć serwisową producenta na terenie Polski. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia produktu w postaci oświadczenia producenta.
2. Wykonawca w składanej ofercie musi przedstawić nazwę producenta i nazwę oferowanego urządzenia.
3. Wszystkie funkcjonalności wymienione w SOPZ są wymaganiami minimalnymi.

Dostarczony przedmiot zamówienia musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się, aby elementy wchodzące w skład przedmiotu zamówienia były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej, Wykonawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Zamawiający wykorzystuje aktualnie system ochrony sieci i bezpiecznych tuneli VPN oparty na rozwiązaniu Fortinet Fortigate300C/Fortigate90D/FortiAnalyzer100C, który zamierza rozbudować o dodatkowe urządzenia sieciowe wyspecyfikowane poniżej.

II ZAKRES ZAMÓWIENIA

I. Dla elementów systemu ochrony sieci i bezpiecznych tuneli VPN obsługujących Generalną Dyrekcję Ochrony Środowiska Wykonawca zapewni wszystkie poniższe funkcjonalności:

1. W przypadku przedmiotu zamówienia pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – system musi posiadać możliwość łączenia w klaster Active-Active lub Active-Passive. W ramach postępowania przedmiot zamówienia musi zostać dostarczony w postaci klastra HA.
2. Przedmiot zamówienia musi posiadać funkcjonalność monitoringu i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Przedmiot zamówienia musi posiadać funkcjonalność monitoringu stanu realizowanych połączeń VPN.

4. Przedmiot zamówienia realizujący funkcję Firewall musi posiadać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. Przedmiot zamówienia realizujący funkcję Firewall musi dysponować minimum 12 portami Ethernet 10/100/1000 Base-TX, 12 gniazdami SFP 1Gbps oraz 2 gniazdami 10G SFP+.
6. Przedmiot zamówienia musi umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 10 milionów jednoczesnych połączeń oraz 270 tysięcy nowych połączeń na sekundę.
8. Przepustowość Firewall'a: nie mniej niż 46 Gbps.
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 22 Gbps.
10. Przedmiot zamówienia realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
11. W ramach dostarczonego przedmiotu zamówienia muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    1) kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
    2) ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
    3) poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
    4) ochrona przed atakami - Intrusion Prevention System.
    5) kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    6) kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP.
    7) kontrola pasma oraz ruchu (QoS, Traffic shaping) – co najmniej określanie maksymalnej i gwarantowanej ilości pasma.
    8) kontrola aplikacji – system musi rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów).
    9) możliwość analizy ruchu szyfrowanego protokołem SSL.
    10) mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 8 Gbps.
13. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 2,4 Gbps.
14. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    1) tworzenie połączeń w topologii Site-to-site oraz Client-to-site.
    2) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    3) praca w topologii Hub and Spoke oraz Mesh.
    4) możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF.

5) obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.

15. W ramach funkcji IPSec VPN, SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
16. Przedmiot zamówienia musi zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
17. Przedmiot zamówienia musi zapewniać możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
18. Przedmiot zamówienia musi zapewniać możliwość translacji adresów NAT adresu źródłowego i docelowego.
19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
20. Przedmiot zamówienia musi posiadać możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
21. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
22. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo system musi umożliwiać wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
23. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
24. Przedmiot zamówienia musi zapewniać dla systemu posiadanie bazy filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy. Administrator musi mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
25. Przedmiot zamówienia musi zapewniać dla systemu posiadanie funkcjonalności automatycznej aktualizacji sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
26. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    1) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    2) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    3) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
    4) rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory.
27. Poszczególne elementy oferowanego przedmiotu zamówienia powinny posiadać następujące certyfikaty:
    1) ICSA lub EAL4 dla funkcji Firewall.

2) ICSA lub NSS Labs dla funkcji IPS.
3) ICSA dla funkcji: SSL VPN, IPSec VPN.

28. Elementy przedmiotu zamówienia muszą posiadać możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
29. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 250 GB, który może być wykorzystany do celów logowania i raportowania. Ponadto system musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze. W ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej o następujących parametrach technicznych:
    1) system logowania i raportowania w formie maszyny wirtualnej musi stanowić centralne repozytorium danych gromadzonych przez urządzenia Zmawiającego (FortiGate, FortiMail, FortiWeb) oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców.
    2) maszyna wirtualna musi mieć możliwość uruchomienia w następujących środowiskach VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure.
    3) obsługa powierzchni dyskowej - minimum 500 GB
    4) obsługa nielimitowanej licencyjnie liczby wirtualnych procesorów.
    5) obsługa nielimitowanej licencyjnie pamięci operacyjnej.
    6) przedmiot zamówienia musi zapewniać:
        a) składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników.
        b) możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci.
        c) kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki.
        d) przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
        e) wyświetlanie nowych logów w czasie rzeczywistym.
        f) analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy.
        g) export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
    7) Przedmiot zamówienia musi zapewniać obsługę przez system Zamawiającego minimum 1 GB spływających logów dziennie.
    8) System musi udostępniać interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH oraz lokalną konsolę tekstową z poziomu środowiska wirtualnego.

30. Serwisy i licencje:
    1) wykonawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa o ważności co najmniej do dnia 31.05.2019 roku. Aktywacja licencji dla funkcji bezpieczeństwa musi nastąpić w ciągu 30 dni od zawarcia umowy.
    2) wykonawca musi zapewnić pierwszą linię wsparcia technicznego telefonicznie w języku polskim w trybie 8x5 co najmniej do dnia 31.05.2019 r.
    3) instalacja oraz konfiguracja, zgodnie z ofertą Wykonawcy, musi być przeprowadzona przez uprawnionych inżynierów Wykonawcy.
31. Gwarancja:
    1) przedmiot zamówienia musi być objęty serwisem gwarancyjnym producenta co najmniej do dnia 31.05.2019 roku, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie systemu w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, Wykonawca przed zawarciem umowy winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
    2) serwis musi być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (Wykonawca przed zawarciem umowy winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy.
    3) w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem zamówienia (tzw. produkty podwójnego zastosowania), Wykonawca winien przed zawarciem umowy 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 2013, poz. 194 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.
    4) wykonawca przed zawarciem umowy winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
32. W zakres przedmiotu zamówienia wchodzi dostawa przedmiotu zamówienia i jego wdrożenie (instalacja i konfiguracja) w miejscu wskazanym przez Zamawiającego. Wykonawca takiej usługi jest zobowiązany do przedstawienia Zamawiającemu przed zawarciem umowy certyfikatów, wystawionych przed producenta oferowanego systemu, dla inżynierów przeprowadzających wdrożenie, które poświadczają zdanie egzaminów i znajomość konfiguracji dostarczonego systemu. Wdrożenie systemu musi obejmować:
    1) wstępną konfigurację i integrację dostarczonego sprzętu z infrastrukturą informatyczną Zamawiającego.
    2) integracja z istniejącym systemem zarządzania.

3) konfiguracja IPSec VPN.
4) konfiguracja polityk firewall.
5) konfiguracja profili UTM.
6) konfiguracja dynamicznego routingu (OSPF).
7) instalacja UTM w miejscu docelowym.
8) testy urządzeń UTM.
9) monitoring.

II. Przedłużenie gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego dla poniżej wymienionych systemów bezpieczeństwa teleinformatycznego Zamawiającego.

1. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja na serwis gwarancyjny i wsparcie producenta, realizowane na terenie Rzeczpospolitej Polskiej, polegające na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy ale nie krócej niż do dnia 31.05.2019 roku subskrypcja dla wszystkich funkcji bezpieczeństwa dla systemu ochrony poczty elektronicznej Zamawiającego: FortiMail 200D (klaster). Aktualne wsparcie i serwis producenta wygasa w dniu 15.11.2017 roku.
2. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 06.10.2018 roku, subskrypcja na serwis gwarancyjny i wsparcie producenta, realizowane na terenie Rzeczpospolitej Polskiej, polegające na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 06.10.2018 roku, subskrypcja dla wszystkich funkcji bezpieczeństwa dla systemu pełniącego funkcję kontrolera sieci bezprzewodowych Zamawiającego: FortiAP 220B (2 sztuki). Aktualne wsparcie i serwis producenta wygasa w dniu 15.05.2018 roku.
3. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja na serwis gwarancyjny i wsparcie producenta, realizowane na terenie Rzeczpospolitej Polskiej, polegające na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja na licencje aktywacyjne dla wszystkich funkcji bezpieczeństwa dla systemu ochrony sieci VPN Zamawiającego: FortiGate 90D (17 sztuk). Aktualne wsparcie i serwis producenta wygasa w dniu 05.11.2018 roku.
4. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja wsparcia producenta dla wszystkich funkcji bezpieczeństwa systemu ochrony poczty elektronicznej Zamawiającego: Fortimail-VM02. Aktualne wsparcie wygasa w dniu 15.10.2018 roku.
5. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja wsparcia producenta dla wszystkich funkcji bezpieczeństwa systemu ochrony poczty elektronicznej Zamawiającego: Fortimail-VM08. Aktualne wsparcie wygasa w dniu 15.05.2019 roku.
6. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja wsparcia producenta dla wszystkich funkcji bezpieczeństwa systemu dwuskładnikowego uwierzytelniania użytkowników Zamawiającego: FortiAuthenticator VM. Aktualne wsparcie wygasa w dniu 30.06.2018 roku.

7. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja na serwis gwarancyjny i wsparcie producenta, realizowane na terenie Rzeczpospolitej Polskiej, polegające na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku, subskrypcja na licencje aktywacyjne dla wszystkich funkcji bezpieczeństwa dla systemu ochrony sieci Zamawiającego: FortiGate 100D (klaster). Aktualne wsparcie i serwis producenta wygasa w dniu 27.11.2017 roku.
8. Dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy ale nie krócej niż do dnia 31.05.2019 roku subskrypcja na serwis gwarancyjny i wsparcie producenta, realizowane na terenie Rzeczpospolitej Polskiej, polegające na naprawie lub wymianie urządzenia w przypadku jego wadliwości oraz dodatkowa przedłużająca na okres zgodny z ofertą Wykonawcy ale nie krócej niż do dnia 31.05.2019 roku subskrypcja na licencje aktywacyjne dla wszystkich funkcji bezpieczeństwa dla systemu ochrony sieci Zamawiającego: FortiWeb 400C (klaster). Aktualne wsparcie i serwis producenta wygasa w dniu 27.11.2017 roku.
9. Wykonawca zobowiązany jest załączyć do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży przedłużania gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego oraz świadczenia usług z nimi związanych.
10. Przed zawarciem umowy w sprawie zamówienia publicznego Wykonawca zobowiązany jest dostarczyć Zamawiającemu oświadczenie producenta lub autoryzowanego dystrybutora producenta informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie Polski.
11. Serwis, o którym mowa w ust. 10, musi być realizowany przez Producenta rozwiązania lub Autoryzowanego Dystrybutora Producenta, mającego swoją lokalizację serwisową na terenie Polski, posiadającego certyfikat ISO 9001 w zakresie usług serwisowych (należy złożyć go na wezwanie Zamawiającego w trybie art. 26 ust. 2 ustawy Pzp).
12. Wykonawca zobowiązany jest zapewnić pierwszą linię wsparcia technicznego, telefonicznie lub poprzez e-mail, w języku polskim w trybie 8 godzin od 9:00 do 17:00, 5 dni w tygodniu (poniedziałek – piątek) na okres zgodny z ofertą Wykonawcy, ale nie krócej niż do dnia 31.05.2019 roku.
13. W przypadku, gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, Wykonawca powinien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej. Zamawiający wymaga, aby dokument powyższy Wykonawca przedłożył przed zawarciem umowy w sprawie zamówienia publicznego.

III. Dostawa 2 sztuk certyfikatów trusted SSL w wariancie Wildcard dla domen *.gdos.gov.pl oraz *.rdos.gov.pl. Wymagania minimalne:

1. rozpoznawany przez 99.00% przeglądarek,
2. szyfrowanie 256 bit,
3. długość klucza szyfrowania 2048 bit,
4. typ walidacji OV,
5. kompatybilny z urządzeniami mobilnymi (smartphony, tablety),

6. gwarancja wystawcy min. 1 000 000 USD,
7. okres ważności 3 lata.