Załącznik nr 2b do zaproszenia
Szczegółowy opis przedmiotu zamówienia – cz. 2

Część 1 – urządzenie do analizowania bezpieczeństwa sieci

Przedmiotem zamówienia jest dostawa fabrycznie nowego urządzenia sieciowego na potrzeby Głównego Urzędu Geodezji i Kartografii. Dostarczone urządzenie jest rozbudową istniejącej infrastruktury sieciowej opartej o urządzenia Fortinet.

Urządzenie do zapisywania zdarzeń, analizy danych przekazywanych z różnych urządzeń firmy Fortinet i innych narzędzi kompatybilnych z serwerem SYSLOG oraz raportowania -1szt.:

FortiAnalyzer-200F PN: FAZ-200F plus FortiGuard dla FortiAnalyzer 200F na 1 rok lub równoważne, urządzenie musi spełniać niżej wskazane minimalne wymagania.

Lp	Minimalne parametry
1.	1. System musi dysponować co najmniej: 2 portami Gigabit Ethernet RJ-45. 2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB. 3. Urządzenie musi być w pełni kompatybilne z urządzeniami UTM firmy Fortinet oraz innymi narzędziami kompatybilnymi z serwerem SYSLOG.
2.	1. System musi być w stanie przyjmować minimum 100 GB logów na dzień. 2. System musi być w stanie przeanalizować minimum 3000 logów na sekundę. 3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 150 systemów.
4.	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. listę najczęściej wykrywanych ataków, b. listę najbardziej aktywnych użytkowników, c. listę najczęściej wykorzystywanych aplikacji, d. listę najczęściej odwiedzanych stron www, e. listę krajów , do których nawiązywane są połączenia, f. listę najczęściej wykorzystywanych polityk Firewall, g. informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem

	UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
5.	W zakresie raportowania system musi zapewniać: 1) generowanie raportów co najmniej w formatach: HTML, PDF, CSV, 2) predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników, 3) funkcję definiowania własnych raportów, 4) możliwość spolszczenia raportów, 5) generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
6.	W zakresie korelacji zdarzeń system musi zapewniać: 1) korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany, 2) konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa, 3) wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware, • Aplikacje sieciowe, • Email, • IPS, • Traffic, • Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.
7.	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. 2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 3. System musi umożliwiać definiowanie co najmniej 6 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
8.	1. Okres gwarancji: 12 miesięcy, licząc od dnia podpisania protokołu odbioru przez Strony umowy – bez zastrzeżeń. 2. Wykonawca dostarczy urządzenie objęte gwarancją producenta lub autoryzowanego dystrybutora urządzania na Polskę.
9.	1) w okresie gwarancji Wykonawca zobowiązuje się do zapewnienia ciągłości realizacji serwisu gwarancyjnego w siedzibie Zamawiającego, na warunkach określonych w pkt 2-9, 2) gwarancja obejmuje naprawę urządzenia przez producenta lub autoryzowanego partnera serwisowego producenta urządzenia, 3) Zamawiający będzie zgłaszał awarie w dni robocze w godzinach 8.15-16.15 – telefonicznie, za pośrednictwem poczty e-mail lub strony internetowej; przyjmowanie

	zgłoszeń serwisowych musi odbywać się w języku polskim, 4) w przypadku zgłoszenia przez Zamawiającego awarii urządzenia, Wykonawca przystąpi do usuwania awarii nie później niż w ciągu następnego dnia roboczego licząc od momentu otrzymania zgłoszenia, 5) Wykonawca maksymalnie w ciągu 2 dni roboczych od momentu otrzymania zgłoszenia, dokona skutecznej naprawy urządzenia; zgłoszenie w trybie 8x5xNBD, 6) w przypadku niemożności naprawy urządzenia w terminie, o którym mowa w pkt 5, Wykonawca dostarczy Zamawiającemu najpóźniej w 2 dniu roboczym od zgłoszenia awarii, na własny koszt, urządzenie o parametrach nie gorszych od urządzenia zaoferowanego, oraz o porównywalnej funkcjonalności; urządzenie zastępcze musi zostać skonfigurowane tak, jak urządzenie użytkowane przez Zamawiającego; urządzenie zastępcze zostanie zwrócone Wykonawcy po zakończeniu naprawy; Zamawiającemu nie przysługuje wówczas kara umowna, o której mowa w § 9 ust. 3 umowy, 7) Wykonawca zobowiązany będzie do wymiany urządzenia na nowe, na własny koszt, w terminie 7 dni roboczych, od dnia zgłoszenia przez Zamawiającego takiego żądania w formie pisemnej, w przypadkach: a) niewykonania naprawy w terminie 5 dni roboczych, od dnia zgłoszenia awarii przez Zamawiającego, b) wystąpienia kolejnej awarii, wady lub usterki urządzenia, po wcześniejszym wykonaniu 3 napraw gwarancyjnych danego urządzenia.

Dodatkowe wymagania przedmiotowe:

a. Podmiot, który będzie świadczył serwis gwarancyjny urządzeń musi posiadać autoryzację producenta urządzenia – dokument potwierdzający spełnianie wymogu należy załączyć do oferty; dokument musi zawierać nazwę (firmę) podmiotu świadczącego serwis gwarancyjny urządzenia,
b. Oferując rozwiązanie równoważne do rozwiązania wskazanego przez Zamawiającego, Wykonawca zobowiązany jest wykazać, że rozwiązanie równoważne spełnia wszystkie wymagania, przy zachowaniu cech technicznych, funkcjonalnych i jakościowych urządzenia. Przez wykazanie równoważności Zamawiający rozumie wykonanie stosownych porównań i analiz, których wyniki należy załączyć do oferty. Zamawiający wymaga dostarczenia urządzenia w postaci komercyjnych platform sprzętowych.
c. Wykonawca dostarczy sprzęt będący przedmiotem zamówienia do siedziby Zamawiającego pod adresem: Główny Urząd Geodezji i Kartografii, ul. Jana Olbrachta 94b, 01-102 Warszawa