Załącznik nr 1 do Umowy nr … z dnia ……

SPECYFIKACJA TECHNICZNA

CZĘŚĆ I PRZEDMIOTU ZAMÓWIENIA

(urządzenia bezpieczeństwa)

OBLIGATORYJNE WYMAGANIA TECHNICZNE

Urządzenie bezpieczeństwa
Urządzenie bezpieczeństwa typ UB1: Imperva X2500 Web Application Firewall lub równoważne, Liczba sztuk: 1

Oferowany model * …….. **Producent * ……..**

Lp.	Opis wymagań minimalnych		Liczba sztuk	Deklaracja zgodności z obligatoryjnymi wymaganiami minimalnymi (np. TAK / NIE)	Różnice / Uwagi / Oferowany sprzęt
1	SS-WAF-X25-H1	X2500 Web Application Firewall	1		
2	SS-WAF-X25-H1-SL0	X2500 Web Application Firewall 1 year standard support	1		
3	SS-M15-H1	M150 Management Server	1		
4	SS-M15-H1-SL0	M150 Management Server 1 year standard support	1		

lub urządzenie(-a) równoważne, spełniające poniższe wymagania minimalne:

1. System zabezpieczeń musi składać się z następujących komponentów:
   a. Moduł wykonawczy
   b. Serwer zarządzania

Tabela 1. Wymagania na moduł wykonawczy

Lp.	Parametr	Wymagania techniczne
1.	Wymagane tryby pracy	Nie mniej niż: • Transparent In-line (warstwa 2 ISO/OSI) • Transparent Reverse Proxy • Reverse Proxy • Sniffing
2.	Ilość/rodzaj portów	Nie mniej niż 6 portów 1Gb Ethernet, w tym 2 porty do zarządzania
3.	Wydajność	• Przepływność nie mniejsza niż 500Mbps • Nie mniej niż 22 000 transakcji HTTP na sekundę
4.	Funkcjonalność zapewniająca niezawodność	Nie mniej niż: • Wbudowany fizyczny bypass dla interfejsów inspekcyjnych • Możliwość redundancji urządzeń dla każdego z trybów pracy systemu przedstawionych w punkcie 1 tabeli 1
5.	Obudowa	Przeznaczona do zamontowania w szafie 19”. Wysokość nie większa niż 2U
6.	Zasilanie i wentylacja	Zasilanie z sieci 100-240V/50-60Hz
7.	Konfiguracja wstępna i zarządzanie	Konfiguracja wstępna (umożliwiająca uwierzytelnienie modułu wykonawczego na serwerze zarządzania) poprzez terminal i linię komend, zarządzanie musi odbywać się wyłącznie poprzez centralny serwer zarządzania

Tabela 2. Wymagania na serwer zarządzania

Lp.	Parametr	Wymagania techniczne
1.	Ilość/rodzaj portów	Nie mniej niż 2 porty 1Gb Ethernet
2.	Obudowa	Przeznaczona do zamontowania w szafie 19”. Wysokość nie większa niż 2U
3.	Zasilanie i wentylacja	Zasilanie z sieci 100-240V/50-60Hz
4.	Konfiguracja wstępna i zarządzanie	Konfiguracja wstępna poprzez terminal i linię komend, zarządzanie musi odbywać się poprzez interfejs przeglądarki internetowej

2. System zabezpieczeń musi zawierać nie mniej niż następujące mechanizmy ochrony:
    a. Stateful Firewall
    b. Weryfikacja zgodności komunikacji sieciowej ze standardem protokołu TCP/IP, opisanym w RFC
    c. Sieciowy system ochrony przed intruzami bazujący na sygnaturach ataków. Wymagane są sygnatury dla nie mniej niż:
        i. Sieci
        ii. Aplikacji Web
        iii. Zapytań Web
    d. Wykrywanie znanych oraz nieznanych robaków sieciowych poprzez analizę heurystyczną
    e. Automatyczne tworzenie i aktualizowanie profili aplikacji Web oraz wykrywanie przy ich użyciu naruszeń bezpieczeństwa. Profil aplikacji Web musi być budowany w sposób automatyczny poprzez analizę ruchu sieciowego. Musi istnieć możliwość automatycznej aktualizacji profilu w przypadku wystąpienia zmiany w strukturze aplikacji. Profil musi uwzględniać nie mniej niż następujące elementy: katalogi, URL-e, cookies, metody dostępu, parametry, typy znaków oraz wartości minimalne/maksymalne wpisywane przez użytkowników w poszczególnych polach formularza. Dodatkowo system musi posiadać możliwość sprawdzenia, które z wykorzystywanych pól są typu „read-only" i nie mogą być zmieniane przez klientów.
    f. Wykrywanie złożonych ataków poprzez mechanizm korelacji wielu zdarzeń. Mechanizm musi umożliwiać definiowanie reguł polityki bezpieczeństwa przy uwzględnieniu co najmniej następujących kryteriów: nagłówki http, źródłowy adres IP, identyfikator sesji lub nazwy użytkownika, ilość wystąpień w określonym takcie czasu, elementy aplikacji (URL-e, parametry), nazwa aplikacji klienta, akceptowany język przeglądarki, rozmiar zwróconej strony oraz czas odpowiedzi serwera Web.
3. Wszystkie wymienione w punkcie 2 funkcje muszą być dostępne w obrębie jednej licencji producenta
4. System musi posiadać możliwość rozbudowy funkcji poprzez zakup dodatkowej licencji producenta. Musi ona uwzględniać mechanizmy opisane w punkcie 2 oraz dodatkowo zawierać nie mniej niż następujące funkcje:
    a. Definiowanie reguł dostępu użytkowników bazodanowych do poszczególnych obiektów w bazie danych poprzez automatyczne tworzenie listy użytkowników oraz listy zapytań sql, jakie użytkownik może wykonać w odniesieniu do tabel baz danych. System musi posiadać dodatkowo możliwość automatycznego tworzenia list: źródłowych adresów IP, nazw aplikacji klienckich oraz nazw systemu operacyjnego, z których użytkownik ma dostęp do zasobów. Na podstawie powyższych list definiowane są reguły polityki bezpieczeństwa.
    b. Tworzenie list tabel, do których poszczególni użytkownicy bazodanowi nie mogą mieć dostępu. Musi istnieć również możliwość definiowania dni tygodnia oraz godzin, w jakich dany użytkownik może nawiązać połączenie z bazą danych.
    c. Monitorowanie oraz rejestrowanie aktywności użytkowników na bazach danych (przy wykorzystaniu języków DDL, DML, DCL). System musi posiadać możliwość monitorowania połączeń użytkowników bezpośrednio z bazą, połączenia przez serwery aplikacyjne oraz obsługę przechowywanych w bazie danych procedur, wywoływanych wraz z parametrami przez klientów. W rejestrowanych zdarzeniach wymagane są co najmniej: nazwa użytkownika aplikacyjnego oraz identyfikator sesji (jeżeli

komunikacja odbywa się przy wykorzystaniu aplikacji Web oraz użytkownik uwierzytelnił się w systemie), źródłowy adres IP, pełne zapytanie SQL wykonane przez użytkownika oraz ilość rekordów zwróconych z bazy danych użytkownikowi. Musi istnieć opcja rejestracji wszystkich rekordów zwróconych przez bazę danych użytkownikowi systemu dla danej reguły monitorowania aktywności. Monitorowanie aktywności użytkowników nie może obniżać wydajności bazy danych i musi odbywać się wyłącznie na podstawie analizy ruchu sieciowego bez konieczności komunikacji systemu zabezpieczeń z bazą danych

   d. Testowanie podatności systemów bazodanowych, przy uwzględnieniu: wykrywania komercyjnych baz danych w sieci korporacyjnej, analiza podatności systemu operacyjnego oraz bazy danych na znane typy ataków, sprawdzenie dostępności nowych wersji systemów bazodanowych oraz weryfikacja zabezpieczenia kont użytkowników bazodanowych. Rozwiązanie musi posiadać funkcję uwierzytelnienia się w systemie operacyjnym oraz w bazie danych w celu wykonania powyższych testów.

5. W przypadku zakupu licencji z punktu 4 system musi zabezpieczać bazy danych nie mniej niż następujących producentów: Oracle, Microsoft, Sybase, Informix, IBM, MySQL. Jako zabezpieczenie rozumiana jest zarówno analiza negatywna jak i pozytywna.
6. W przypadku zakupu licencji z punktu 4 producent musi dostarczyć darmowe aplikacje agentów instalowanych na serwerach bazodanowych, w celu rejestrowania lokalnej aktywności użytkowników. Wspierane muszą być co najmniej następujące systemy operacyjne: Linux, Windows. Aplikacja agenta ma na celu wysyłanie informacji o lokalnej aktywności użytkowników do modułu wykonawczego. Moduł wykonawczy musi posiadać możliwość weryfikacji stanu działania agenta.
7. Rozwiązanie musi posiadać możliwość rejestrowania naruszeń bezpieczeństwa oraz udostępniać administratorom co najmniej następujące informacje o zdarzeniach: nazwa użytkownika aplikacyjnego (jeżeli klient zalogował się w systemie przez aplikację Web) oraz pełny nagłówek http przesłany do serwera aplikacji Web. Musi istnieć możliwość rejestrowania kodu źródłowego strony zwracanej klientowi przez aplikację Web.
8. System musi posiadać mechanizm ochrony oraz profilowania serwisów Web, uwzględniając elementy XML oraz akcje SOAP.
9. System musi analizować zarówno zapytania http jak i odpowiedzi w celu wykrycia nadużyć oraz wycieków danych niejawnych
10. System musi posiadać następujące metody reakcji na incydenty:
    a. W trybie In-line:
        i. Blokowanie pakietu
        ii. Blokowanie źródła ataku w postaci adresu IP, nazwy użytkownika lub sesji (jeżeli użytkownik uwierzytelnił się w systemie)
    b. W trybie nasłuchu:
        i. Wysyłanie pakietu TCP RST do klienta oraz serwera
11. Rozwiązanie musi posiadać funkcję wysyłania informacji o zdarzeniach poprzez protokół SNMP, syslog oraz wiadomość e-mail
12. System musi posiadać predefiniowane raporty dotyczące:
    a. Alarmów bezpieczeństwa
    b. Zdarzeń systemowych
    c. Zmian w profilach aplikacji

13. Musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej
14. Rozwiązanie musi posiadać funkcję korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For", umożliwiającą identyfikację w alarmach zabezpieczeń oryginalnego adresu źródłowego w przypadku wdrożenia systemu za serwerem typu Proxy
15. Producent musi zapewnić aktualizację systemu, uwzględniając co najmniej: sygnatury ataków, listę reguł polityki oraz listę raportów.
16. W celu zapewnienia aktualności systemu zabezpieczeń wymagana jest możliwość automatycznego oraz ręcznego pobierania aktualizacji. Aktualizacje muszą zawierać co najmniej: sygnatury ataków, raporty bezpieczeństwa, testy podatności systemów. Dodatkowo musi istnieć również możliwość wykorzystania Proxy do aktualizacji.
17. System musi posiadać możliwość integracji z komercyjnymi skanerami zabezpieczeń IBM AppScan oraz HP WebInspect. Integracja ma na celu zautomatyzowanie procesu definiowania reguł polityki bezpieczeństwa bazujących na wynikach działania skanera zabezpieczeń. Powyższa funkcja nie może wymagać zakupu dodatkowych licencji.
18. Pracując w trybie transparentnym In-line moduł wykonawczy musi gwarantować opóźnienie nie większe niż 1 milisekunda w celu zapewnienia wysokiej wydajności chronionych usług.
19. Zarówno moduł wykonawczy jak i serwer zarządzania muszą posiadać redundantne dyski twarde oraz zasilanie.
20. System zabezpieczeń musi umożliwiać funkcjonowanie w architekturze klastra modułów wykonawczych, pracującego w trybie active – backup. Konfiguracja oraz zarządzanie klastrem musi odbywać się poprzez centralny moduł zarządzania.
21. Wymagana jest pojemność dysku twardego serwera zarządzania nie mniejsza niż 300GB, modułu wykonawczego nie mniejsza niż 500 GB
22. Zarządzanie systemem musi odbywać się poprzez interfejs przeglądarki Web w celu eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora
23. Całość konfiguracji oraz repozytorium logów musi być przechowywane na dostarczanym serwerze zarządzania. Pojemność dyskowa serwera zarządzania musi umożliwiać przechowywanie logów przez co najmniej 6 miesięcy.
24. Wymagane jest zarządzanie zorientowane zadaniowo. Oznacza to, iż musi istnieć mechanizm informowania administratora o wykonaniu/nie wykonaniu na czas zadania zleconego innym użytkownikom systemu.
25. Wszystkie elementy systemu zabezpieczeń muszą być dostarczone przez jednego producenta w formie dedykowanych urządzeń sieciowych (ang. appliance)
26. Wymagane jest wsparcie techniczne producenta, uwzględniające aktualizacje bazy sygnatur, wsparcie w rozwiązywaniu problemów technicznych (telefonicznie lub w przypadku wystąpienia takiej konieczności w miejscu zainstalowania sprzętu)

b) Inne wymagania

1. Wykonawca dokona przeszkolenia 3 administratorów Zamawiającego z zakresu podstawowej oraz zaawansowanej konfiguracji dostarczanego urządzenia bezpieczeństwa typ UB1 w autoryzowanym przez dostawcę sprzętu ośrodku szkoleniowym. Szkolenia powinny trwać co najmniej 5 dni roboczych. Ze względu na wykonywane przez wyznaczonych pracowników obowiązki, szkolenia powinny obywać się w dwóch terminach dla grupy 2 – osobowej oraz dla 1 administratora. Zamawiający dopuszcza szkolenia w systemie otwartym.
2. Wykonawca dokona montażu urządzeń w wskazanej przez Zamawiającego szafie teletechnicznej.
3. Wykonawca dokona wstępnej konfiguracji urządzeń zgodnie ze wskazaniami Zamawiającego
4. Wykonawca wykona dokumentację powdrożeniową.

SPECYFIKACJA TECHNICZNA

CZĘŚĆ I PRZEDMIOTU ZAMÓWIENIA

(urządzenia bezpieczeństwa)

OBLIGATORYJNE WYMAGANIA TECHNICZNE

Urządzenie bezpieczeństwa typ UB2 CISCO ASA 5520 lub równoważne, Liczba sztuk: 2

Oferowany model * …….. **Producent * ……..**

Lp.	Opis wymagań minimalnych		Liczba sztuk	Deklaracja zgodności z obligatoryjnymi wymaganiami minimalnymi (np. TAK / NIE)	Różnice / Uwagi / Oferowany sprzęt
1	ASA5520-AIP10-K9	ASA 5520 Appliance w/ AIP-SSM-10, SW, HA, 4GE+1FE, 3DES/AES	1		
2	CAB-ACE	Power Cord Europe	1		
3	SF-ASA-8.0-K8	ASA 5500 Series Software v8.0	1		
4	ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	1		
5	Included: ASA5520-VPN-PL	ASA 5520 VPN Plus 750 Peer License	1		
6	Included: ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	1		

7	Included: SF-ASA-AIP-6.0-K9	ASA 5500 Series AIP Sofware 6.0 for Security Service Modules	1		
8	Included: ASA-180W-PWR-AC	ASA 180W AC Power Supply	1		
9	Included: ASA-AIP-10-INC-K9	ASA 5500 AIP Security Services Module-10 included w/ bundles	1		
10	Included: ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	1		
11	CON-CSSPD-ASAINC10	SHARED SUPP SDS AIP SSM-10 included in ASA systems	3		
12	CON-CSSPD-AS2A10K9	SHARED SUPP SDS ASA5520 w AIP-SSM-10, 4GE+1FE, 3DES/AES	3		
13	CON-SUSA-AS2A10K9	IPS Signature Only (3 lata)	1		

lub urządzenie(-a) równoważne, spełniające poniższe wymagania minimalne:

1. Urządzenie musi pełnić rolę zapory ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
2. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
3. Urządzenie musi posiadać co najmniej 4 porty 10/100/1000Base-T GigabitEthernet oraz 1 porty 10/100Base-T FastEthernet
4. Urządzenie musi dedykowane dwa porty: dla podłączenia konsoli oraz dla uzyskania zdalnego dostępu przez modem asynchroniczny
5. Urządzenie musi posiadać co najmniej 2 porty USB dla przyszłych zastosowań,
6. Urządzenie musi posiadać co najmniej 512 MB DRAM oraz 64 MB Flash
7. Urządzenie musi posiadać dodatkowy slot pozwalający na wykorzystanie modułów funkcjonalnych,
8. Urządzenie musi posiadać moduł pełnej funkcjonalności systemu IPS (Intrusion Prevention System) ASA5520-AIP10-K9 lub równoważny. Moduł ten musi posiadać następujące funkcje:
   - umożliwienie pracy w trybie IPS (In-line);
   - wykrywanie ataków oparciu o sygnatury oraz o wykrywanie anomalii (w oparciu np. o tzw. Micro Engines)

- posiadanie zakodowanych co najmniej 2300 sygnatur ataków
- możliwość definicji reakcji z dokładnością do jednej sygnatury
- grupowanie sygnatur ataków
- tworzenia zdarzeń opisanych przez naruszenie kilku niezależnych sygnatur ataku
- określenie znaczenia ataku na podstawie kilku zmiennych w szczególności: znaczenia atakowanego systemu, znaczenia naruszonej sygnatury oraz prawdopodobieństwa ataku.
- umożliwianie indywidualnego (przez administratora) definiowania poziomu zagrożenia dla sygnatury
- posiadanie mechanizmu notyfikacji administratora o zaistniałym ataku (co najmniej przez e-mail)
- zarządzanie przez linię komend, graficznie przez przeglądarkę internetową oraz musi być dostępna dedykowana aplikacja;
- konsola zarządzająca musi pracować na platformie Windows NT/XP/W2K – należy przewidzieć narzędzie umożliwiające zarządzanie 5-cioma sondami lub więcej;

10. Urządzenie musi posiadać możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
11. Urządzenie musi posiadać umożliwienie terminowanie co najmniej 750 jednoczesnych sesji VPN opartych o protokół IPSec
12. Urządzenie musi posiadać możliwość terminowania jednocześnie 750 sesji WebVPN
13. Urządzenie musi obsługiwać co najmniej 280000 jednoczesnych sesji/połączeń.
14. Przepustowość obsługiwana przez urządzenie nie może być mniejsza niż 440 Mbps i jednocześnie 220 Mbps dla ruchu szyfrowanego symetrycznymi algorytmami 3DES/AES
15. Przepustowość urządzenia przy jednoczesnym włączeniu usług zapory ogniowej oraz IPS musi być wyższa niż 220 Mbps przy zastosowaniu odpowiedniego modułu funkcjonalnego
16. Urządzenie musi posiadać umożliwienie obsługi co najmniej 150 VLAN;
17. Urządzenie musi posiadać umożliwienie implementacji redundancji funkcji failover typu Active/Standby;
18. Urządzenie musi posiadać umożliwienie wirtualizacji konfiguracji – należy dostarczyć licencję na 5 wirtualnych instancji;
19. Urządzenie musi umożliwić inspekcję ruchu Voice w zakresie protokołów H.323, SIP, MGCP, TAPI, JTAPI
20. Urządzenie musi umożliwić blokowanie aplikacji typu „internetowy komunikator" wykorzystujących port 80 (np.: Skype, MSN)
21. Urządzenie musi umożliwić translację adresów sieciowych NAT – zarówno dla ruchu wchodzącego, jak i wychodzącego, obsługę protokołów OSPF, RIP.
22. Urządzenie musi umożliwić blokowanie aplikacji typu peer-to-peer (np: Kaaza, eDonkey)
23. Urządzenie musi umożliwić analizę protokołów HTTP oraz FTP na portach innych niż standartowe

24. Urządzenie musi być zarządzane przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.
25. Urządzenie musi być przystosowane do montażu w szafie rackowej 19" i nie zajmować więcej miejsca niż 1RU
26. Urządzenie musi być objęte 36 miesięczną gwarancją i wsparciem technicznym w siedzibie użytkownika licząc od dnia podpisania protokołu odbioru jakościowego dla dostawy.

b) Inne wymagania

1. Wykonawca dostarczy 30 sztuk kabli UTP kat6 o długości 1 m
2. Wykonawca dostarczy 30 sztuk kabli UTP kat6 o długości 2 m
3. Wykonawca dostarczy 30 sztuk kabli UTP kat6 o długości 3 m

UWAGI ZAMAWIAJĄCEGO:

(*) Należy podać oferowany model i nazwę producenta oferowanego sprzętu.

....., dnia, ...
Miejscowość Data

.....
Podpis(-y) osoby(osób) wskazanej(-ych)
w dokumencie uprawniającym do występowania
w obrocie prawnym lub posiadającej(-ych) pełnomocnictwo(-a).
(Zalecany czytelny podpis(-y) lub podpis(-y) i pieczątka(-i) z imieniem i nazwiskiem).