Załącznik nr 1b do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

A. Urządzenie typu firewall spełniające następujące funkcjonalności:

1. Musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.
2. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
3. Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.
4. Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
5. Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
6. Obsługa dla IPv6.
7. Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
8. Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.
9. Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.
10. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
11. Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
12. Firewall musi działać w następujących trybach:
    a. routera (tzn. w warstwie 3 modelu OSI),
    b. przełącznika (w warstwie 2 modelu OSI),
    c. transparentnym
    d. pasywnego nasłuchu.

    Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.
13. Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie

wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.

14. Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
15. Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.
16. Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
17. Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
18. Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.
19. Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
20. Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.
21. Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
22. Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.
23. Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
24. Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.
25. Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.

26. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.
27. Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.
28. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.
29. Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).
30. Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.
31. Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
32. Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.
33. Urządzenie musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu.
34. Rozwiązanie musi umożliwiać rozbudowę o możliwość wykrywania domen DGA i ruchu tunelowanego przez DNS. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres **minimum 60 miesięcy**.
35. Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku, gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
36. Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST,

blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.

37. Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
38. Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.
39. Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
40. Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s
41. Firewall musi posiadać przepustowość w ruchu nie mniej niż 4,5 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 2,5 Gbps.
42. Urządzenie musi obsłużyć minimum 400 000 jednoczesnych sesji oraz 70 000 nowych połączeń na sekundę.
43. Urządzenie musi zapewniać wydajność przynajmniej 3 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.
44. Urządzenie musi być przystosowane do montażu w szafie rack. W ramach postępowania należy dostarczyć półkę do szafy Rack 19” pod zaoferowane urządzenia.
45. Urządzenie musi być wyposażone w redundantne zasilacze.
46. Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.
47. Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
48. Musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
49. Urządzenie musi zapewniać zestawienie przynajmniej 1500 sesji SSL VPN.
50. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów.

51. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN.
52. Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres **60 miesięcy**.
53. Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres **60 miesięcy**.
54. Firewall musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres **60 miesięcy**.
55. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
56. Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres **60 miesięcy.**
57. Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na okres 60 miesięcy.**
58. Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.
59. Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders" raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls" w raportach opublikowanych w przeciągu 2 ostatnich lat.

60. Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
61. Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
62. Urządzenie nie może znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
63. Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przez okres **60 miesięcy.**
64. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.
65. W ramach postępowania należy dostarczyć dwa identyczne urządzenia, przy czym jedno z urządzeń będzie działało jako główne (aktywne) a drugie będzie pełniło rolę urządzenia zapasowego. Po przełączeniu na urządzenie zapasowe poziom ochrony musi być dokładnie taki sam jak na firewallu głównym (musi działać ten sam zestaw licencji).

B. Warunki serwisu technicznego i procedura zgłoszeń:

1. Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.
2. Wsparcie techniczne musi być świadczone przez okres **60 miesięcy**.
3. W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego.
4. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.
5. Procedura zgłaszania awarii lub wad sprzętu została opisana w § 9 ust. 4 wzoru umowy.

C. Zakres szkolenia:

1. Konfigurowanie zasad haseł, dostępu oraz kont administratorskich do urządzenia.
2. Konfigurowanie interfejsu do zarządzania (oznaczony jako mgmt).
3. Założenie kont suportowych na portalu producenta oraz na portalu dystrybutora.
4. Pobranie licencji na urządzenie.
5. Zaktualizowanie oprogramowania sprzętowego, bazy sygnatur, aplikacji i zagrożeń.
6. Konfigurowanie interfejsów z adresacją publiczną.
7. Konfigurowanie interfejsów z adresacją prywatną.
8. Konfigurowanie interfejsów, z których można zarządzać firewallem.
9. Konfigurowanie interfejsów do połączenia klastra HA firewalla.

10. Konfigurowanie redundancji połączeń WAN, jeśli występują min. dwa łącza operatorskie.
11. Konfigurowanie odpowiednich stref bezpieczeństwa (Zony).
12. Konfigurowanie DNS.
13. Konfigurowanie serwera(ów) DHCP oraz NTP.
14. Konfigurowanie statycznych wpisów przydzielanych adresów z puli DHCP.
15. Konfigurowanie statycznych wpisów tabeli routingu.
16. Konfigurowanie polityk QoS.
17. Dodanie odpowiednich wpisów obiektowych (Adresów IP, Grup, Aplikacji, Grup Aplikacji oraz Serwisów wraz z grupowaniem).
18. Dodanie Tagów wykorzystywanych przy dalszej konfiguracji dla czytelności ustawień.
19. Konfigurowanie profilu Antywirusa.
20. Konfigurowanie profilu anty-Spyware.
21. Konfigurowanie profilu ochrony podatności.
22. Konfigurowanie profilu filtrowania URL.
23. Konfigurowanie profilu blokowania plików.
24. Konfigurowanie profilu analizy sandboxowej.
25. Stworzenie grup profili bezpieczeństwa.
26. Ustawienie User ID (po wdrożeniu AD).
27. Utworzenie wymaganych polityk bezpieczeństwa.
28. Utworzenie polityk bezpieczeństwa z uwzględnieniem funkcji: Threat Prevention, sandbox i przewidywania zagrożeń nieznanych, , bezpieczeństwa DNS.
29. Konfiguracja reguł pozwalających na rozszywanie ruchu ssl. Demonstracja na wybranych hostach, zostawienie narzędzi i skryptów pozwalających na rozszerzenie zakresu urządzeń objętych daną regułą.
30. Utworzenie wymaganych polityk translacji adresów IP (NAT) - SNAT i DNAT.
31. Wygenerowanie wymaganych certyfikatów pod VPN i rozszywanie SSL.
32. Ustawienie tunelu VPN do połączeń typu klient – serwer (standardowo jeden portal i brama).
33. Konfiguracja tunelu IPsec dla tunelu site – to – site.
34. Podłączenie urządzenia docelowego i zweryfikowanie poprawności działania wdrożonej konfiguracji.
35. Konfigurowanie generowania raportów i wysyłania ich na wskazany e-mail.
36. Dokumentacja powdrożeniowa zawierająca podsumowanie i zestawienie z wyżej wymienionych zagadnień objętych usługą wdrożenia.