Załącznik Nr 1b do SIWZ
jednocześnie Załącznik nr 1 do Umowy

Opis przedmiotu zamówienia - Część II

Zawiera minimalne wymagania dla pary urządzeń

Całość rozwiązania musi pochodzić i być zarządzana centralnym systemem jednego (tego samego) producenta.

1. Para urządzeń typu NG Firewall – system HA

1. System musi być dostarczony jako specjalizowane urządzenia sieciowe (appliance) pracujące w modelu klastra wysokiej dostępności. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active oraz aby każde z urządzeń potrafiło pracować niezależnie z zachowaniem wszystkich funkcjonalności.
2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części („ćwiartce) Leaders w edycji aktualnej na dzień składania ofert.
3. Dostarczone urządzenia NG Firewall:
   - muszą być obsługiwane przez posiadany przez Zamawiającego system zarządzania Panorama
   - muszą pozwalać na uruchomienie rozproszonego klastrowania z wykorzystywanymi przez Zamawiającego urządzeniami 5200 producenta Palo Alto.
   - muszą umożliwiać wykorzystanie pozyskanych danych rozpoznawania użytkowników przez posiadane przez Zamawiającego urządzenia NG Firewall i realizować obustronną wymianę danych – odczytywać oraz aktualizować nowe dane o rozpoznanych użytkownikach.
4. System musi umożliwiać działanie w następujących trybach pracy
   a) rutera (tzn. w warstwie 3 modelu OSI),
   b) przełącznika (tzn. w warstwie 2 modelu OSI),
   c) w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)
   d) w trybie pasywnego nasłuchu (sniffer/tap). System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. System musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i instancje systemu zabezpieczeń (w zakresie VPN, Firewall, IPS, Routing). Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF dla IPv4 i IPv6.
6. System musi być wyposażony w co najmniej następujące interfejsy sieciowe
   a) 4 porty RJ-45 100Mbps + 4 porty RJ-45 1G/10G, lub 4 porty RJ-45 100M/1G/10G
   b) 16 portów 1G/10G akceptujących wkładki SFP oraz SFP+
   c) 4 porty 40G akceptujących wkładki QSFP+
   d) 1 port 40G akceptujący wkładki QSFP+ na potrzeby HA.
7. System musi być wyposażony w co najmniej jeden port konsoli oraz w co najmniej jeden dedykowany port zarządzający.
8. Urządzenie NG Firewall musi posiadać budowę z odseparowanymi procesorami zarządzającymi (tzw. Management) od procesorów przetwarzających ruch sieciowy (tzw. Data Plane). Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może wpływać

na pogorszenie funkcjonowania części zarządzającej (m.in. nie może powodować opóźnień, problemów z konfigurowaniem czy monitorowaniem urządzenia, reakcją GUI i CLI).
9. System musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Podinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
10. System musi posiadać przepustowość ruchu co najmniej 8 Gbit/s dla kontroli zawartości tj.: firewall, kontrola aplikacji na wszystkich portach, IPS, antywirus, antymalware lub antyspyware, z włączoną kontrolą/filtrowaniem typów plików. Wydajność IPSec VPN urządzenie musi wynosić co najmniej 11 Gbit/s.
11. System musi obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 175 000 połączeń na sekundę.
12. System musi posiadać co najmniej 2 redundantne zasilacze umożliwiające podłączenie urządzenia do sieci energetycznej 230V.
13. System zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
14. Polityka zabezpieczeń firewall musi uwzględniać
    a) adresy IP klientów i serwerów,
    b) protokoły i usługi sieciowe,
    c) aplikacje,
    d) kategorie URL,
    e) użytkowników aplikacji i grupy,
    f) reakcje zabezpieczeń,
    g) rejestrowanie zdarzeń i alarmowanie
    h) zarządzanie pasmem w sieci w oparciu o
        i. priorytet,
        ii. pasmo gwarantowane,
        iii. pasmo maksymalne,
    i) interfejs wejściowy i wyjściowy
15. System musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
16. System musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu (bez użycia zewnętrznych narzędzi).
17. System musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi,.lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie metadanych pliku.

18. System musi zapewniać DNS sinkholing.

19. System musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
    a) Active Directory,
    b) Terminal Services
20. System musi pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
Musi być możliwe tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

Musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
21. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
22. System 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 oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
23. System musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
24. System musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
25. System musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN).
26. System musi wykonywać zarządzanie pasmem sieci (QoS) i ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego.
27. System musi posiadać funkcję filtrowania URL.
28. System musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja/polityka oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb - bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
29. System musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
30. System musi posiadać moduł antymalware lub antyspyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
31. System musi umożliwiać wykrywanie i blokowania ataków DNS - wykrywający i blokujący ruch do domen uznanych za złośliwe.
32. Zarządzanie systemem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
33. System musi być wyposażony w interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji – należy dostarczyć licencję na 20 użytkowników.
34. 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.
35. System bezpieczeństwa musi umożliwiać uwierzytelniania administratorów za pomocą nie mniej niż: baza lokalna oraz serwer Radius/TACACS+.
36. System musi pozwalać na selektywne wysyłanie logów bazując na ich rodzaju.
37. Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
38. Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania SSH.
39. Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet – AntiBot.
40. Funkcjonalność zabezpieczania DNS dostępna na urządzeniu musi umożliwiać procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja), tunelowania DNS. Urządzenia muszą posiadać ciągły (on-line) dostęp do

centralnego repozytorium zagrożeń DNS, który będzie wykorzystywany w procesie decyzyjnym funkcjonalności.
41. Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox" plików różnych typów przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Aktualizacja musi być realizowana w ciągu maksymalnie 15 minut a system umożliwiać ciągłą aktualizację w trybie real-time.
Funkcja przesyłania do systemu Sandbox musi umożliwiać analizę plików następujących typów: Android (APK, DEX z APK), MacOSX (Mach-O, DMG, PKG), Skrypty (JS, VBS,PowerShell, BAT),Flash, aplety Java (JAR/class), PDF, RAR, 7ZIP, Linux ELF, PE/ Portable Executable (EXE, DLL, FON).
42. Moduł filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Wymagane jest posiadanie oddzielnych kategorii dla zagrożeń typu malware, phishing, command-and-control oraz ostatnio zarejestrowane domeny (NRD). Równolegle z oceną URL musi być dokonywany i określany poziom ryzyka związany z danym URL na poziomie małe ryzyko, średnie ryzyko, wysokie ryzyko.
43. Zamawiający dopuszcza by funkcja ręcznego tworzenia sygnatur (IPS) była realizowana bezpośrednio na urządzeniu lub na konsoli zarządzającej.
44. Zamawiający wymaga następujących funkcjonalności wraz z niezbędnymi subskrypcjami/licencjami, jeśli są one konieczne. Jeżeli funkcjonalność licencjonowana jest na ilość użytkowników należy dostarczyć ilości dla maksymalnych pojemności oferowanego urządzenia:
a) IPS, Antywirus, Kontrola aplikacji, Antymalware, Antyspyware
b) Bezpieczeństwo DNS
c) Sandboxing
45. Konieczność współdzielenia sygnatur Malware/IPS oraz kategorii URL między istniejącymi NG FW a nowymi w celu zachowania spójnej polityki bezpieczeństwa.
46. Zamawiający wymaga dostępności interfejsu API dla oferowanych urządzeń NG Firewall, który odwzorowuje funkcje interfejsów CLI oraz GUI, celem zapewnienia otwartości systemu pod kątem innych integracji oraz automatyzacji.
47. Dostarczane subskrypcje, gwarancje na nie mniej niż **36** miesięcy

Wraz z urządzeniami wymagane jest dostarczenie kompatybilnych wkładek światłowodowych (lista dla pary HA):
a) 2 gotowe kabel połączeniowe SFP+ 10G (tzw. kabel DAC/AOC) minimum 5m długości.
b) 1 gotowy kabel połączeniowy QSFP+ 40G (tzw. kabel DAC/AOC) minimum 5m długości.
c) 4 gotowe kabel połączeniowe SFP+ 10G (tzw. kabel DAC/AOC) minimum 5m długości.
d) 8 wkładek QSFP+ 40GBASE-BiDi
e) 8 wkładek SFP+ 10GBASE-SR

Usługa wsparcia technicznego - gwarancja
Wymagane jest dostarczenie wsparcia producenta na okres minimum 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.