

# OPIS PRZEDMIOTU ZAMÓWIENIA

## Zakup i przedłużenie subskrypcji oraz usług serwisowych dla urządzeń firmy Palo Alto Networks

1. Przedmiotem zamówienia jest zakup i przedłużenie subskrypcji oraz usług serwisowych dla urządzeń firmy Palo Alto Networks zaimplementowanych w infrastrukturze Zamawiającego.
2. W ramach zamówienia Wykonawca zapewni asystę techniczną do etapu poprawnego powiązania subskrypcji będących przedmiotem zamówienia na wskazanych urządzeniach zamawiającego
3. Zamawiający wymaga aby subskrypcje i usługi serwisowe producenta dla urządzeń typu pierwszego oraz trzeciego były świadczone przez okres 39 miesięcy, a dla urządzeń typu drugiego przez okres 36 miesięcy. Dodatkowo, subskrypcja dla Systemu Centralnego Zarządzania Panorama również powinna być świadczona przez okres 39 miesięcy. Celem Zamawiającego jest zrównanie terminów zakończenia wszystkich subskrypcji i usług serwisowych.
4. Wykonawca ma obowiązek zapewnić usługi serwisowe producenta które muszą obejmować:
  - diagnostykę zdarzeń dotyczących oprogramowania;
  - dostarczanie rozwiązań błędów oprogramowania;
  - zapewnienie łat (ang. patches), tj. poprawek lub aktualizacji mających na celu usunięcie problemów, błędów, rozszerzenie funkcjonalności lub zwiększenie wydajności wcześniejszej wersji oprogramowania;
  - zapewnienie aktualizacji do nowych, wyższych wersji oprogramowania (ang. upgrades);
  - udzielanie odpowiedzi na zapytania związane z instalacją i eksploatacją dostarczonego oprogramowania;
  - aktualizacje bazy aplikacji;
  - procedurę wymiany sprzętu na nowy w przypadku awarii (RMA)
5. Subskrypcje dla urządzeń **typu pierwszego** (2 urządzenia PA-5220) muszą obejmować minimum:
  - a. Aktualizacje baz sygnatur IPS,
  - b. Aktualizacje baz sygnatur AV,
  - c. Aktualizacje baz sygnatur AntiSpyware,
  - d. Aktualizacje baz dla podstawowej ochrony DNS,
  - e. Aktualizacje/dostęp do bazy URL z kategoryzacją stron WWW,
  - f. Analizę zagrożeń typu 0-day w systemem Sandbox,
  - g. Wymóg realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN),
  - h. Kontrolę tuneli client-to-site w oparciu o analizę stanu hosta (profilowanie stanu hosta) w ramach systemów operacyjnych Windows, MacOS, Android, Linux, iOS,
  - i. Zaawansowaną ochronę DNS w trybie rzeczywistym. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę

domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej:

- wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 30 milionów wpisów.
- możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
- wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)
- wykrywanie domen dynamicznych Dynamic DNS
- wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych
- domen fast flux.

6. Subskrypcje dla urządzeń **typu drugiego** (2 urządzenia PA-5220) muszą obejmować minimum:

- a. Aktualizacje baz sygnatur IPS,
  - b. Aktualizacje baz sygnatur AV,
  - c. Aktualizacje baz sygnatur AntiSpyware,
  - d. Aktualizacje baz dla podstawowej ochrony DNS,
  - e. Aktualizacje/dostęp do bazy URL z kategoryzacją stron WWW,
  - f. Analizę zagrożeń typu 0-day w systemem Sandbox,
  - g. Wymóg realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN),
  - h. Kontrolę tuneli client-to-site w oparciu o analizę stanu hosta (profilowanie stanu hosta) w ramach systemów operacyjnych Windows, MacOS, Android, Linux, iOS,
  - i. Zaawansowaną ochronę DNS w trybie rzeczywistym. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej:
- wykrywanie zapytań do domen złośliwych. Baza domen musi mieć co najmniej 30 milionów wpisów.
  - możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
  - wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)
  - wykrywanie domen dynamicznych Dynamic DNS
  - wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych
  - domen fast flux.

7. Subskrypcje dla urządzeń **typu trzeciego** (2 urządzenia PA-3220) muszą obejmować minimum:

- a. Aktualizacje baz sygnatur IPS,
- b. Aktualizacje baz sygnatur AV,
- c. Aktualizacje baz sygnatur AntiSpyware,
- d. Aktualizacje baz dla podstawowej ochrony DNS,
- e. Aktualizacje/dostęp do bazy URL z kategoryzacją stron WWW,
- f. Analizę zagrożeń typu 0-day w systemem Sandbox,
- g. Wymóg realizacji sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN),

8. Subskrypcja dla Systemu Centralnego Zarządzania urządzeniami NGFW.

Zamawiający posiada w swojej infrastrukturze system do Centralnego Zarządzania firewallami o nazwie Palo Alto Networks Panorama, który zarządza posiadanymi klastrami urządzeń PA-5220 oraz PA-3220. Zamawiający wymaga, aby w ramach oferty uwzględnić zakup usługi wsparcia na system Centralnego Zarządzania Panorama. Oferta wsparcia dla Systemu Centralnego Zarządzania należy zapewnić na okres 39 miesięcy, w oparciu o usługę określaną jako wsparcie partnerskie, opisaną kodem producenta jako PAN-SVC-BKLN-PRA-25-3YR-R – Partner enabled premium support 3 year term renewal, Panorama 25 devices

9. Zestawienie modeli wraz z numerami seryjnymi oraz wymaganymi w zamówieniu serwisami i subskrypcjami prezentuje tabela:

Klaster urządzeń PA-5220 – urządzenia typu pierwszego		
Numer seryjny urządzenia	013201022788	013201022724
Wymagane wsparcie i subskrypcje w postaci numerów produktowych/ PN	PAN-PA-5220-TP-3YR-HA2-R	PAN-PA-5220-TP-3YR-HA2-R
	PAN-PA-5220-WF-3YR-HA2-R	PAN-PA-5220-WF-3YR-HA2-R
	PAN-PA-5220-ADVURL-3YR-HA2-R	PAN-PA-5220-ADVURL-3YR-HA2-R
	PAN-PA-5220-GP-3YR-HA2	PAN-PA-5220-GP-3YR-HA2
	PAN-PA-5220-DNS-3YR-HA2	PAN-PA-5220-DNS-3YR-HA2
	PAN-SVC-BKLN-5220-3YR-R	PAN-SVC-BKLN-5220-3YR-R
Klaster urządzeń PA-5220 – urządzenia typu drugiego		
Numer seryjny urządzenia	013201025627	013201025647
Wymagane wsparcie i subskrypcje w postaci numerów produktowych/ PN	PAN-PA-5220-TP-3YR-HA2-R	PAN-PA-5220-TP-3YR-HA2-R
	PAN-PA-5220-WF-3YR-HA2	PAN-PA-5220-WF-3YR-HA2-R
	PAN-PA-5220-ADVURL-3YR-HA2-R	PAN-PA-5220-ADVURL-3YR-HA2-R
	PAN-PA-5220-GP-3YR-HA2	PAN-PA-5220-GP-3YR-HA2
	PAN-PA-5220-DNS-3YR-HA2-R	PAN-PA-5220-DNS-3YR-HA2-R
	PAN-SVC-BKLN-5220-3YR-R	PAN-SVC-BKLN-5220-3YR-R
Klaster urządzeń PA-3220 – urządzenia typu trzeciego		
Numer seryjny urządzenia	016201024151	016201024154
Wymagane wsparcie i subskrypcje w postaci numerów produktowych/ PN	PAN-PA-3220-TP-3YR-HA2-R	PAN-PA-3220-TP-3YR-HA2-R
	PAN-PA-3220-WF-3YR-HA2-R	PAN-PA-3220-WF-3YR-HA2-R
	PAN-PA-3220-ADVURL-3YR-HA2-R	PAN-PA-3220-ADVURL-3YR-HA2-R
	PAN-SVC-BKLN-3220-3YR-R	PAN-SVC-BKLN-3220-3YR-R
System Centralnego Zarządzania Panorama		
Wymagane wsparcie i subskrypcje w postaci numerów produktowych/ PN	PAN-SVC-BKLN-PRA-25-3YR-R – system centralnego zarządzania winien umożliwiać zarządzanie oraz kolekcję logów z minimum 25 urządzeń fizycznych	

Numerы produktowe przedstawione w tabeli posiadają charakter orientacyjny, odnosząc się do subskrypcji na okres 36 miesięcy. Przedmiotem niniejszego zamówienia jest dostarczenie oficjalnych odpowiedników wskazanych numerów produktowych, które będą dostosowane do specyficznych wymagań czasowych dla różnych typów urządzeń. Dla urządzeń typu pierwszego i trzeciego wraz z

Systemem Centralnego Zarządzania Panorama, subskrypcje oraz usługi serwisowe są wymagane na okres 39 miesięcy, natomiast dla urządzeń typu drugiego wymagany jest standardowy okres subskrypcji wynoszący 36 miesięcy.