ZP/35/2022

Zał. nr 2 do SWZ

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa licencji wraz z 5-cio letnim wsparciem technicznym oraz sygnatur bezpieczeństwa dla wdrożonego w Uniwersytecie Medycznym w Łodzi klastra urządzeń klasy firewall, opartego o urządzenia Palo Alto PA-5250 zarządzanego za pośrednictwem centralnej konsoli zarządzania – Panorama.

Dostawa obejmuje:

Lp.	Part number	Opis
I	PAN-P A-5250-TP-5YR-HA2-R (przedłużenie licencji posiadanej przez zamawiającego)	Threat prevention subscription 5 year prepaid renewal for device in an HA pair, PA-5250
II	PAN-SVC-BKLN-5250-5YR-R – (5-letnie wsparcie techniczne i rozszerzenie gwarancji)	Partner enabled premium support 5-year prepaid renewal, PA-5250
III	PAN-SVC-BKLN-PRA-25-5YR-R – (wsparcie dla centralnej konsoli zarządzania – Panorama)	Partner enabled premium support 5 year prepaid renewal, Panorama 25 devices

Na podstawie dostarczonej licencji wsparcia technicznego oraz aktualizacji sygnatur bezpieczeństwa Wykonawca zapewnia Zamawiającemu przez okres 60 miesięcy liczonych od daty wygaśnięcia poprzedniej licencji, tj. od 25.05.2022r., :

1. Wsparcie techniczne i gwarancję – (dotyczy licencji wskazanej w pkt. II) (zwane dalej wsparciem) świadczone przez autoryzowane przez producenta centrum serwisowe niezależne od Integratora/Wykonawcy i realizowane we współpracy z producentem posiadanego przez zamawiającego klastra urządzeń klasy firewall.

Wsparcie obejmuje:

a. Dostęp do Centrum Wsparcia Technicznego (TAC) przez: stronę internetową, email oraz telefonicznie w języku polskim

b. Wsparcie przy rozwiązywaniu problemów związanych z działaniem NGFW w trybie 24x7,

   i. czas reakcji na zgłoszony drogą mailową lub telefoniczną problem –

      1. maks. 1 godzina w przypadku zdarzeń krytycznych (np. uszkodzenie urządzenia) zgłoszonych telefonicznie

      2. maks. 8 godzin w przypadku pozostałych zgłoszeń

   ii. przy wystąpieniu awarii urządzenia, któregokolwiek z jego komponentów lub wyposażenia, w tym modułów optycznych – wymiana lub naprawa (RMA)

      1. w terminie NBD (następny dzień roboczy) przy zgłoszeniu awarii do godziny 15:00 w dniu roboczym

      2. w ciągu dwóch dni roboczych przy zgłoszeniu awarii po godzinie 15:00 w dniu roboczym

c. Dostęp (tj. uprawnienie do pobierania i instalowania) do wszystkich aktualizacji dotyczących oprogramowania systemowego (PANOS) wydawanych przez Producenta.

d. Dostęp (tj. uprawnienie do pobierania i instalowania) do wszystkich aktualizacji dotyczących bazy danych aplikacji (App ID) wydawanych przez Producenta.

e. Dostęp (tj. uprawnienie do pobierania i instalowania) do wszystkich aktualizacji dotyczących klienta sieci VPN (Global Protect) wydawanych przez Producenta

f. Dostęp do bazy wiedzy producenta - w języku polskim lub angielskim w tym do:

   i. dokumentacji producenta dotyczącej instalacji, konfiguracji i utrzymania urządzeń

   ii. przewodników konfiguracyjnych

   iii. not dotyczących wersji oprogramowania systemowego (tzw. release notes)

   iv. odpowiedzi na najczęściej zadawane pytania (tzw. FAQ)

   v. baz danych ze sposobami rozwiązywania typowych problemów

Ponadto:

g. W przypadku wymiany urządzenia, któregokolwiek z jego komponentów lub wyposażenia, w tym modułów optycznych – wymiana następuje na sprzęt tożsamy lub

równoważny (w przypadku gdy producent dokonałby zmian w swoim portfolio produktowym)

h. W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki pozostają w całości u zamawiajacego. Nie są konieczne działania np. w postaci demontażu dysku i pozostawienia u zamawiającego fragmentów dysku z nośnikami danych.

2. Subskrypcję Threat Prevention (zwaną dalej Threat Prevention lub TP) zapewniającą wszystkie opisane poniżej funkcje. Subskrypcja TP jest realizowana przez producenta

W ramach subskrypcji (dotyczy licencji wskazanej w pkt. I) Threat Prevention dostarczane są aktualizacje (w postaci sygnatur lub cyklicznych update'ów) dla następujących funkcji:

a. Aktualizacje baz sygnatur silnika/modułu IPS
b. Aktualizacje baz sygnatur silnika/modułu AV
c. Aktualizacje baz sygnatur dla silnika/modułu AntySpyware
d. Możliwość współpracy z systemem sandbox dla plików wykonywalnych
e. Aktualizacje bazy określającej najbardziej złośliwe domeny w ramach podstawowej ochrony DNS

Subskrypcja Threat Prevention (wraz ze wsparciem technicznym) dla posiadanych przez Uniwersytet Medyczny w Łodzi urządzeń PA-5250 pozwala na uzyskanie poniższych kluczowych funkcji:

a. Ochrona realizowana przez moduł inspekcji antywirusowej uruchamiany per aplikacja. Baza sygnatur anty-wirus jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny
b. Ochrona realizowana przez moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI - IPS/IDS. Baza sygnatur IPS/IDS jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny
c. Ochrona realizowana przez moduł antyspyware. Baza sygnatur antyspyware jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny
d. Podstawowa ochrona DNS realizowana w zakresie
    i. wykrywania zapytań do domen złośliwych.

ii. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)

e. Wykrywanie aktywności sieci typu Botnet na podstawie analizy behawioralnej

f. Współpraca z chmurowym systemem sandbox (Wildfire) znajdującym się w chmurze obliczeniowej producenta Firewall'a- możliwość wysyłania plików wykonywalnych przesyłanych przez urządzenie do analizy i korzystanie z aktualizacji systemu NGFW. Wildfire na podstawie przeprowadzonej analizy, może zaktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik.

g. Możliwość blokowania transmisji wskazanych plików do/od określonych grup użytkowników np. plików pakietu biurowego, plików szyfrowanych, wykonywalnych itp. – uruchamiane per aplikacja.

h. Deszyfracja wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (wsparcie dla TLSv1.1, TLSv1.2 i TLSv1.3). Odszyfrowany ruch (a nie jego kopia) może zostać przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do firewalla, w celu jego dalszego przetwarzania.

i. Wbudowana i automatycznie aktualizowana przez producenta lista serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika lub stosowania mechanizmu "certificate pinning").

j. Inspekcja szyfrowanej komunikacji SSH-w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

k. Ochrona przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

l. Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.

m. Inspekcja (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa.

n. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN.

o. obsługa do 30000 tuneli/użytkowników z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW.

p. Oprogramowanie klienta VPN (bez konieczności dokupienia dodatkowej licencji) jest dostępne dla systemów operacyjnych Windows i MacOS

q. Oprogramowanie klienta VPN jest objęte wsparciem producenta w okresie zgodnym z długością wsparcia dla firewalla.

r. Możliwość automatycznego pobierania z zewnętrznych systemów atrybutów w postaci adresów IP, grup adresów, nazw DNS oraz stron www (URL) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.