Wydatek współfinansowany z Europejskiego Funduszu Społecznego

Obsługa serwisowa i wsparcie na okres 12 miesięcy dla dwóch posiadanych przez Zamawiającego urządzeń Next Generation Firewall

Zamawiający posiada urządzenia:

Lp.	Opis urządzenia NGF	Typ pracy	Numer seryjny
1.	Palo Alto PA-3020	Klaster HA	001801028920
2.	Palo Alto PA-3020		001801028921

z aktywnymi subskrypcjami do dnia 16 marca 2019 r.:

- PAN-PA-3020-TP-HA2 (Threat prevention subscription for devices in HA pair),
- PAN-PA-3020-URL4-HA2 (PANDB URL filtering for device in an HA pair),
- PAN-SVC-BKLN-3020 (Partner enabled premium support).

Wszystkie nazwy własne produktów i licencji użytych w niniejszym dokumencie dotyczą infrastruktury będącej w posiadaniu Zamawiającego. Dostawa urządzeń oraz oprogramowania wskazanych w formie nazw handlowych nie jest przedmiotem niniejszego postępowania.

1. W ramach wsparcia Wykonawca przedłuży posiadane przez Zamawiającego subskrypcje dla dwóch urządzeń Palo Alto PA-3020 działających w klastrze HA w okresie od dnia zawarcia umowy na okres 12 miesięcy:
   a) PAN-PA-3020-TP-HA2 (Threat prevention subscription for devices in HA pair),
   b) PAN-PA-3020-URL4-HA2 (PANDB URL filtering for device in an HA pair),
   c) PAN-SVC-BKLN-3020 (Partner enabled premium support).

2. W ramach wsparcia, o którym mowa w pkt 1, Zamawiający otrzyma możliwość korzystania z następujących usług świadczonych przez producenta:
   a) aktualizacji oprogramowania firmware do najnowszych wersji publikowanych przez producenta,
   b) aktualizacji bazy wirusów,
   c) aktualizacji bazy definicji IPS (Intrusion Prevention System),
   d) aktualizacji bazy sygnatur anty-spyware,
   e) aktualizacji sygnatur aplikacji,
   f) dostępu do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych,
   g) pomocy technicznej.

3. W ramach obsługi serwisowej, Wykonawca udzieli gwarancji na urządzenia NGF Zamawiającego.

4. Gwarancja producenta będzie spełniać następujące warunki:
   a) wszelkie koszty usunięcia awarii (usług, części, sprzętu zastępczego i transportu) ponosi producent sprzętu lub autoryzowana przez niego firma serwisująca, przy czym poprzez awarię Zamawiający rozumie problem w prawidłowym funkcjonowaniu całej infrastruktury sieciowej bądź pojedynczego urządzenia całkowicie uniemożliwiający pracę systemu lub pojedynczego urządzenia. Awaria zgłaszana będzie drogą telefoniczną, a następnie potwierdzona za pomocą poczty elektronicznej,

b) czas reakcji serwisu: najpóźniej do końca następnego dnia roboczego (tj. dnia, który nie jest dniem ustawowo wolnym od pracy w rozumieniu ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy, Dz. U. z 2015 r., poz. 90, oraz sobót) od chwili dokonania zgłoszenia,
c) przyjmowanie zgłoszeń w godzinach 8.00-16.00 w dni robocze drogą telefoniczną bądź za pomocą poczty elektronicznej,
d) czas usunięcia awarii, tj. przywrócenia pełnej funkcjonalności całej infrastruktury sieciowej bądź pojedynczego urządzenia, w terminie maksymalnie do 3 dni roboczych od chwili dokonania zgłoszenia przez Zamawiającego (ostateczny termin wynikać będzie z oferty Wykonawcy),
e) w przypadku awarii jednego z urządzeń trwającej dłużej niż 3 dni roboczych lub w przypadku wystąpienia jednoczesnej awarii obydwu urządzeń działających w klastrze Wykonawca zobowiązany jest niezwłocznie (tego samego dnia w przypadku awarii zgłoszonych do godziny 13.00, a w przypadku awarii zgłoszonych po godz. 13.00 następnego dnia) udostępnić podłączyć i skonfigurować na ten okres sprzęt o wydajności i funkcjonalności nie gorszej niż sprzęt uszkodzony, a w przypadku klastra urządzeń o parametrach – pozwalających na przywrócenie pełnej funkcjonalności klastra,
f) wszelkie koszty usunięcia awarii (usług, części, sprzętu zastępczego i transportu) ponosi producent sprzętu lub autoryzowana przez niego firma serwisująca, przy czym poprzez awarię Zamawiający rozumie problem w prawidłowym funkcjonowaniu całej infrastruktury sieciowej bądź pojedynczego urządzenia całkowicie uniemożliwiający pracę systemu lub pojedynczego urządzenia.

5. W przypadku, gdy Wykonawca oferuje subskrypcje i wsparcie nie w pełni kompatybilne z urządzeniami NGF posiadanymi przez Zamawiającego, Zamawiający dopuszcza zaoferowanie w ramach wynagrodzenia subskrypcji i wsparcia wraz z klastrem urządzeń NGF posiadającym nie gorszą funkcjonalność niż urządzenia NGF posiadane przez Zamawiającego:

   System zabezpieczeń NGF jest to dedykowane urządzenie zabezpieczeń sieciowych (appliance) w postaci klastra wysokiej dostępności (HA - High Availability) złożonego z dwóch identycznych urządzeń pracujących w trybie Active-Passive, z możliwością przełączenia na tryb Active-Active. W architekturze sprzętowej systemu występuje separacja modułu zarządzania (control-plane) i modułu przetwarzania danych (data-plane). Całość sprzętu i oprogramowania jest wspierana przez jednego producenta.

   5.1 Wymagania szczegółowe dotyczące systemu zabezpieczeń NGF:
   a) brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej,
   b) przepływność w ruchu full-duplex na poziomie 2 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, 1 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługa 250 000 jednoczesnych połączeń,
   c) 12 portów Ethernet 10/100/1000, możliwość zamontowania w urządzeniu 8 interfejsów optycznych SFP,
   d) działanie w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując 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. Tryb pracy zabezpieczeń jest ustalany w konfiguracji interfejsów inspekcyjnych. Możliwość pracy w różnych trybach jednocześnie, w pojedynczej logicznej instancji systemu zabezpieczeń (np. wirtualny system, wirtualna domena, itp.), możliwość pracy w trybie transparentnym L1 (bez konieczności nadawania adresu IP) oraz pozwala na tworzenie transparentnych subinterfejsów, które będą obsługiwały ruch z wybranych vlanów lub podsieci IP,
   e) obsługa protokołu Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3, urządzenie obsługuje 4094 znaczników VLAN,

f) obsługa 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwia uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie obsługuje protokoły routingu dynamicznego: BGP, RIP i OSPF,
g) zgodna z ustaloną polityką kontrola ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji,
h) możliwość uwzględniania w polityce zabezpieczeń firewall stref bezpieczeństwa, adresów IP klientów i serwerów, protokołów i usług sieciowych, aplikacji, użytkowników aplikacji, reakcji zabezpieczeń, rejestrowania zdarzeń i alarmowania oraz zarządzania pasmem sieci (priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ),
i) możliwość działania zgodnego z zasadą „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone,
j) automatyczne identyfikowanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji odbywa się poprzez sygnatury i analizę heurystyczną. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji jest taka sama i wynosi w ruchu full-duplex 2 Gbit/s. Zezwolenie dostępu do aplikacji odbywa się w regułach polityki firewall (tzn. reguła firewall posiada oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalne:
   - aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall lub inny silnik zaimplementowany na urządzeniu NGF;
   - kontrola aplikacji w modułach innych jak firewall;
   - kontrola aplikacji wymagająca konfiguracji dodatkowego modułu zabezpieczeń innego niż firewall,
k) wykrywanie aplikacji takich jak Skype, Tor, BitTorrent, eMule, UltraSurf, wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

5.2 System zabezpieczeń NGF zapewnia możliwość:
a) ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta,
b) definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Istnieje możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie,
c) blokowania transmisji plików: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku odbywa się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia,
d) ochrony przed atakami typu „Drive-by-download" poprzez konfigurację strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików,
e) inspekcji 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 posiada możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL,
f) inspekcji komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System posiada możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji: wykrywanie

i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL,

g) inspekcji szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH,
h) transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości odbywa się również transparentnie. Ponadto system posiada możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników,
i) zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia,
j) uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering jest przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiada nie mniej niż 20 milionów rekordów URL,
k) uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa),
l) ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta,
m) automatycznego pobierania listy stron WWW z zewnętrznego systemu w określonych przedziałach czasu i używania ich w politykach bezpieczeństwa,
n) uruchomienia modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń,
o) uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa),
p) uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS jest przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń,
q) uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa),
r) ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta,
s) uruchomienia modułu anty-spyware bez konieczności dokupowania jakichkolwiek komponentów sprzętowych, poza subskrypcją. Moduł anty-spyware jest osobno licencjonowanym modułem, ale bez ograniczenia ilości obsługiwanych użytkowników, reguł, czy hostów w sieci. Baza sygnatur anty-spyware jest przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co producent systemu zabezpieczeń,
t) uruchomienia modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa),

u) ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

5.3 System zabezpieczeń NGF posiada:

a) sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe,
b) funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem,
c) funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej,
d) funkcjonalność statycznej i dynamicznej translacji adresów NAT. Mechanizmy NAT umożliwiają dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet,
e) funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP,
f) możliwość zestawiania zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN odbywa się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych odbywa się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji,
g) możliwość konfiguracji 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). Istnieje możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci. Do realizacji zadania dopuszczalne jest zainstalowanie dedykowanego agenta (aplikacji) na serwerach ActiveDirectory lub integracja z systemem zabezpieczeń typu NAC/802.1x
h) możliwość zarządzania pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System umożliwia stworzenie 8 klas dla różnego rodzaju ruchu sieciowego,
i) możliwość integracji ze środowiskiem wirtualnym VMware w taki sposób, aby firewall automatycznie pobierał informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie pociąga za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla,
j) możliwość zarządzania z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem,
k) interfejs XML API lub JANG lub RestAPI, będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI),
l) zabezpieczenie kryptograficzne (poprzez szyfrowanie komunikacji) dostępu do urządzenia i zarządzania nim z sieci. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach, uwierzytelniania administratorów za pomocą:
   - bazy lokalnej,
   - serwera LDAP,
   - RADIUS,
   - Kerberos lub TACACS;

stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS)

m) wbudowany twardy dysk lub pamięć flash do przechowywania logów i raportów o pojemności 120 GB SSD. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie może być wymagany do zapewnienia tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia,
n) możliwość konfigurowania różnych serwerów Syslog per polityka bezpieczeństwa. Dopuszczalna jest wykorzystanie dodatkowego redundantnego klastra HA (2 appliance, maksymalnie 2U w szafie 19”), realizującego funkcje syslog-proxy zgodnie z wymogiem
o) możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane zawierają informacje o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www,
p) możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów jest dostępny w formatach: PDF, CSV i XML,
q) możliwość stworzenia raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni (nie mniej niż 3),
r) możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub ActiveActive.

5.4 Moduł ochrony przed awariami monitoruje i wykrywa uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.