

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest odnowienie wsparcia technicznego i subskrypcji dla posiadanego przez Dyрекcję Generalną Lasów Państwowych w Warszawie (zwaną dalej DGLP w Warszawie) oprogramowania Check Point, zarejestrowanego u producenta na koncie klienta nr **6289517**.

W ramach zamówienia Wykonawca zobowiązany doprowadzić do uzyskania:

- a) dostępu do usług subskrypcyjnych na poziomie obecnie zawartym w licencjach (tam, gdzie występują, dla usług subskrypcyjnych, których data ważności przypada po 1 grudnia 2021 r. należy przedłużyć ich ważność do 1 grudnia 2022 r.),
- b) dostępu do aktualizacji i poprawek oprogramowania opublikowanych przez producenta,
- c) dostępu do usług wsparcia technicznego producenta na poziomie CPES-CO-Premium,

w okresie od dnia 1 grudnia 2021 roku do dnia 1 grudnia 2022 roku.

Użyte w specyfikacji określenia wskazujące znaki towarowe, patenty lub pochodzenie przedmiotu zamówienia należy odczytywać wraz z wyrazami „lub równoważne”. Wykonawca oferując przedmiot równoważny do opisywanego w specyfikacji jest zobowiązany zachować równoważność w zakresie parametrów użytkowych, funkcjonalnych i jakościowych, które muszą być na poziomie nie niższym od parametrów wskazanych przez DGLP w Warszawie w stosunku do wersji oprogramowania Check Point R81.00.

Produkty równoważne – wymagania:

- 1) funkcjonalność i zakres licencji co najmniej na poziomie produktów znajdujących się na koncie klienta,
- 2) możliwość zarządzania wszystkimi funkcjami całości oprogramowania z serwera Check Point Security Management Sever, na który DGLP w Warszawie posiada już wymagane licencje. Wymaga się aby integracja rozwiązań dotyczyła:
 - logowania zdarzeń,
 - zarządzania konfiguracją Firewall-i oraz klastra,
 - zarządzania politykami bezpieczeństwa,
 - monitorowania, raportowania oraz wykonywania statystyk zarówno z danych historycznych jak i aktualnych (występujących w czasie rzeczywistym),
- 3) Dodatkowym wymaganiem jest kompatybilność z aktualną licencją Check Point oraz z najnowszym oprogramowaniem zalecanym przez producenta (z zachowaniem gwarancji producenta Check Point),
- 4) możliwość pracy Firewall-i na oddzielnych serwerach w trybie 64-bit na platformie Check Point GAIA w klastrze obciążeniowym pracującym w trybie równoważenia obciążenia (Load Sharing),
- 5) możliwość pracy systemu zarządzającego na oddzielnym serwerze w trybie 64-bit na platformie Check Point GAIA w środowisku wirtualizacji VMware,
- 6) szyfrowanie komunikacji z Check Point z wykorzystaniem jego mechanizmów szyfrujących,

**Załącznik nr 1
do SWZ DZ.270.89.2021**

- 7) ochrona wewnętrzna sieci lokalnej za pomocą systemu zapory sieciowej (Firewall) dla nielimitowanej liczby urządzeń/adresów IP i użytkowników,
- 8) moduł zarządzania posiadający wewnętrzny, zintegrowany urząd certyfikacji (Certificate Authority),
- 9) możliwość instalacji w architekturze centralnej – na pojedynczym komputerze, lub rozproszonej, trójwarstwowej – na 3 różnych komputerach (moduł Firewall, moduł zarządzania i interfejs GUI),
- 10) możliwość pracy modułów firewall'a w trybie wieloprocessorowym z możliwością przydziału określonej liczby procesorów w ramach posiadanej licencji,
- 11) polityka bezpieczeństwa Firewall w zakresie kontroli ruchu sieciowego uwzględnia kierunek przepływu pakietów, protokoły i usługi sieciowe, użytkowników i serwery usług, stan połączenia oraz dane aplikacyjne (m.in. obsługuje fragmentację IP, ochronę systemu operacyjnego przed atakami Exploit i DoS),
- 12) identyfikowanie niedozwolonych lub podejrzanych działań i prób ataku, a po ich wykryciu podnoszenie alarmu (m.in. wykrywanie skanowania portów, IP Spoofing, SYN Flood, CodeRed, Nimda),
- 13) zapewnienie, bez dodatkowych aplikacji, szczegółowej kontroli aplikacji sieciowych (m.in. kontrola schematów i adresacji URL, kontrola rozmiaru URL, blokada niedozwolonych załączników w stronach HTML, jak ActiveX i Java, blokada niedozwolonych plików kopiowanych przez http, blokada URL zawierających niedozwolone słowa, kontrola rozmiaru przesyłek pocztowych, blokada Mail Relaying, blokada niedozwolonych plików przesyłanych jako załączniki poczty),
- 14) zapewnienie filtrowania treści Web w oparciu o bazę skategoryzowanych URL (dorośli, reklama, sztuka, czat, komputery, przestępczość, narkotyki, edukacja, finanse, jedzenie, gry, moda, rząd, hacking, zdrowie, hobby, praca, dziecinne, motoryzacja, wiadomości, wyszukiwanie fotografii, religia, obchodzenie zabezpieczeń przez Proxy, seks, zakupy, sport, strumienie audio-video, podróże, przemoc, broń, dostęp do e-mail przez WWW) aktualizowanych co najmniej 1 raz dziennie,
- 15) dynamiczna i statyczna translacja adresów NAT (generowanie automatyczne lub definiowanie ręczne reguł NAT),
- 16) zapewnienie komunikacji pomiędzy modulem zabezpieczeń Firewall i modulem zarządzania, szyfrowanej i uwierzytelnionej z użyciem certyfikatów cyfrowych generowanych przez moduł zarządzania,
- 17) zapewnienie szyfrowanej komunikacji pomiędzy interfejsem GUI i modulem zarządzania, uwierzytelnianie administratorów Firewall za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych,
- 18) możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkownikami),
- 19) posiadanie wielu metod uwierzytelniania użytkowników lokalnych i zdalnych (np. uwierzytelnianie przeźroczyste, gdzie Firewall przechwytuje sesję i uwierzytelnia jej użytkownika, uwierzytelnienie za pomocą agenta na stacji użytkownika, uwierzytelnienie po połączeniu się z modulem Firewall) – baza danych przechowywana jest lokalnie na Firewall lub na zewnętrznym serwerze (np. LDAP),
- 20) zarządzanie zabezpieczeniami Firewall, funkcjonującymi w różnych miejscach sieci, z centralnej, graficznej konsoli administratora GUI (polityka bezpieczeństwa wszystkich zabezpieczeń sieci

- tworzy jeden, przejrzysty zbiór reguł , a konsola zarządzania posiada możliwość automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa),
- 21) zintegrowania funkcjonalność zarządzania pasmem w sieci,
 - 22) możliwość rozszerzenia funkcjonalności zabezpieczeń Firewall za pomocą rozwiązań innych dostawców (np. oprogramowanie antywirusowe, urzędy certyfikacji, systemy uwierzytelniania) przy czym integracja Firewall z zabezpieczeniami innych dostawców odbywa się za pomocą dedykowanej technologii OPSEC,
 - 23) tworzenie sieci VPN w oparciu o standard IPSec/IKE, funkcjonujące w trybie site-to-site oraz client-to-site,
 - 24) uwierzytelnianie w sieci VPN za pomocą certyfikatów cyfrowych wydawanych lokalnie oraz przez zewnętrzny urząd certyfikatów,
 - 25) zabezpieczenie danych w sieci VPN z użyciem mocnych algorytmów kryptograficznych (co najmniej AES-256),
 - 26) funkcjonowanie zabezpieczeń Firewall na wielu różnych platformach sprzętowych z dedykowanym przez producenta Firewall systemem operacyjnym i na dedykowanych urządzeniach Appliance,
 - 27) certyfikat bezpieczeństwa Common Criteria EAL4 (oprogramowanie musi posiadać ten certyfikat),
 - 28) zintegrowane QoS,
 - 29) integracja z centralnymi systemami zarządzania i rejestrowania zdarzeń,
 - 30) możliwość obsługi platform otwartych, jak i dedykowanych rozwiązań sprzętowo-programowych za pomocą tego samego oprogramowania różniącego się tylko typem licencji,
 - 31) monitorowanie w czasie rzeczywistym,
 - 32) konsola graficzna do obsługi edycji polityk bezpieczeństwa,
 - 33) centralna dystrybucja oprogramowania i licencji,
 - 34) prawo pobierania:
 - sygnatur do ochrony przed atakami,
 - sygnatur kontroli aplikacyjnej,
 - filtrowania i kategoryzacji URL,przez okres od dnia aktywacji licencji do dnia 1 grudnia 2022 r.
 - 35) wdrożenie dodatkowych produktów w celu zrealizowania wymagań DGLP w Warszawie nie może wiązać się z utratą gwarancji producenta na już posiadane komponenty systemu zabezpieczeń Check Point,
 - 36) mechanizm automatycznego wykrywania oraz blokowania połączeń do sieci typu Botnet,
 - 37) mechanizm automatycznego wykrywania jak i blokowania złośliwego oprogramowania,
 - 38) mechanizm ochrony przed spamem,
 - 39) mechanizm umożliwiającego kontrolę połączeń szyfrowanych typu HTTPS,
 - 40) mechanizm blokowania określonych aplikacji,
 - 41) wdrożony system klastrów firewall-i musi współpracować ze wszystkimi urządzeniami sieciowymi Lasów Państwowych jak również integrować się systemami wspomagającymi zarządzanie bezpieczeństwem,
 - 42) wszelkie koszty zwłaszcza związane ze sprzętem, dostosowaniem, konfiguracją oraz pracami związanymi z wdrożeniem, migracją, dokumentacją powykonawczą, i szkoleniem służb IT oraz w razie konieczności wszystkich pracowników Lasów Państwowych wraz z dostarczeniem

Załącznik nr 1
do SWZ DZ.270.89.2021

materiałów szkoleniowych i dokumentacji powykonawczej, w przypadku zaoferowania rozwiązania równoważnego, ponosi Wykonawca,

- 43) w przypadku rozwiązania równoważnego wsparcie techniczne musi być świadczone na takim samym poziomie CPES-CO-Premium oraz zapewniać DGLP w Warszawie gotowość producenta do świadczenia pomocy w przypadku awarii i problemów technicznych oraz dostępu do poprawek i nowych wersji oprogramowania od dnia aktywacji licencji do dnia 1 grudnia 2022 r,
- 44) na żądanie DGLP w Warszawie, w przypadku zaproponowania rozwiązania równoważnego odnośnie wymaganych funkcjonalności Wykonawca musi osobiście w siedzibie DGLP w Warszawie przeprowadzić testy potwierdzające równoważność zaproponowanego rozwiązania na koszt Wykonawcy.