LOTNICZE POGOTOWIE RATUNKOWE

CENTRALA
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933

Załącznik nr 2c do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Budowa zapasowego ośrodka LPR – zapory sieciowe

Spis treści

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

SŁOWNIKI I SKRÓTY

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Dni robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35.
Informacje	Należy przez to rozumieć informacje, o których mowa w art. 78 ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576).
Oprogramowanie	Oprogramowanie standardowe i oprogramowanie aplikacyjne.
Oprogramowanie standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci. Zamawiający dopuszcza zastosowanie oprogramowania standardowego w poniższych obszarach: 1) system operacyjny; 2) oprogramowanie bazodanowe; 3) oprogramowanie do tworzenia raportów; 4) oprogramowanie do archiwizacji i tworzenia kopii bezpieczeństwa; 5) oprogramowanie antywirusowe; 6) oprogramowanie ETL (ang. Extract, Transform and Load); 7) komunikator (np. oparty o protokół XMPP); 8) oprogramowanie do wirtualizacji; 9) oprogramowanie serwera pocztowego; 10) oprogramowanie serwera aplikacyjnego, kontener aplikacji (z wyłączeniem kodu aplikacji udostępnianej użytkownikowi), serwera WWW; 11) oprogramowanie narzędziowe do monitorowania i diagnozy Systemu; 12) oprogramowanie sterujące i zarządzające centralami telefonicznymi. Zamawiający dopuszcza zastosowanie oprogramowania standardowego, którego producentem jest Wykonawca lub podmiot trzeci również w innych obszarach pod warunkiem, że zastosowanie takiego oprogramowania nie ograniczy kompatybilności z innymi dostępnymi na rynku rozwiązaniami technicznymi oraz dalszej rozbudowy Systemu i świadczenia serwisu gwarancyjnego przez inne podmioty niż Wykonawca i podmiot trzeci , co wymaga przekazania kodów źródłowych oprogramowania standardowego oraz udzielenia licencji dla oprogramowania standardowego na polach eksploatacji określonych w umowie , którego producentem jest Wykonawca lub podmiot trzeci wraz z prawem do modyfikacji kodu źródłowego przez Zamawiającego i osoby trzecie oraz udzielenia zezwolenia na wykonywanie praw zależnych do dokonanych w ten sposób modyfikacji oprogramowania standardowego i jego aktualizacji.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

Skrót/pojęcie	Definicja
	Każde oprogramowanie standardowe musi uzyskać akceptację Zamawiającego.
SLA	Service Level Agreement, poziom dostępności usług.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Urządzenia	Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i odnoszącą się do nich dokumentacją techniczną producenta, w tym również okablowanie strukturalne i szafy rackowe oraz ich wyposażenie, będące przedmiotem niniejszego zamówienia.
Usługa serwisu gwarancyjnego	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania dostarczonych urządzeń i oprogramowania, w szczególności usuwanie błędów.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

CEL ZAMÓWIENIA

Celem zamówienia jest dostawa 2 szt. urządzeń typu **Next Generation Firewall** dla ośrodka zapasowego Lotniczego Pogotowia Ratunkowego.

PRZEDMIOT ZAMÓWIENIA

Zmawiający wymaga dostarczenia pary redundantnej firewalli pełniących rolę „Edge Security" spełniających poniższe wymagania. Zamawiający wymaga również dostarczenia wszystkich wymaganych w opisie licencji oraz rozszerzonego wsparcia serwisowego producenta na okres i zakres zgodnie z wymaganiami opisanymi w pkt. 3 dotyczącym gwarancji i serwisu.
Ilekroć w dokumentacji użyto nazw własnych, znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych – dopuszcza się rozwiązania równoważne.

1) WYMAGANIA WARSTWA FIREWALLI

Nr	Wymagania minimalne
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". Całość sprzętu musi być zarządzana przez jednego producenta.
2	Urządzenie musi być wyposażone w ➢ 4 interfejsy 10/100/1000 (RJ45), ➢ 4 interfejsy 1GE SFP , ➢ 4 interfejsy 10GE SFP+ .

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

3	Urządzenie musi być wyposażone w dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w moduł klasy Lights Out Management (LOM) lub odpowiednik pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania).
4	Urządzenie musi być wyposażone w dysk HDD lub SSD do przechowywania logów i raportów o pojemności nie mniejszej niż 200GB.
5	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: ➢ minimum 2,1 Gbps dla Firewall/kontroli aplikacji, ➢ minimum 1,0 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware, ➢ minimum 13 100 tys. nowych połączeń na sekundę, ➢ minimum 192 000 równoległych sesji. Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych. Jako scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego lub chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.
6	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy: a. rutera (tzn. w warstwie 3 modelu OSI), b. przełącznika (tzn. w warstwie 2 modelu OSI), c. w trybie pasywnego nasłuchu (sniffer).
7	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
8	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
9	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
10	Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

11	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 1,7 Gbps dla IPSEC VPN, Minimum 1 000 tuneli IPSEC VPN (site-to-site), Minimum 1 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (dla Windows, Android, iOS) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 1000 jednoczesnych użytkowników.
12	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej ➢ oznaczania pakietów znacznikami DiffServ, ➢ utworzenia co najmniej 8 klas ruchu sieciowego, ➢ kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.
13	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
14	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
15	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
16	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenie konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
17	Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz obsługę minimum 100 stref bezpieczeństwa.
18	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) 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.
19	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
20	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
21	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
22	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download”.
23	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
24	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

25	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory, b) usługi katalogowe LDAP, c) serwery Terminal Services, d) logi z syslog.
26	Polityka kontroli dostępu urządzenia 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.
27	Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia.
28	Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia. Zamawiający dopuszcza zastosowanie zamiennie do modułu antywirus silnika antymalware opisanego w OPZ jako funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.
29	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem. Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Zamawiający NIE wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

	Licencja na współpracę z sandboxem lokalnym i sandboxem chmurowym jest wymagana, jeżeli zaoferowane rozwiązanie nie posiada dedykowanego silnika antywirusowego.
30	Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia
31	Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). Zamawiający NIE wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia.
32	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet.
33	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia
34	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
35	System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu: a. administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu, b. operator, który ma możliwość tylko odczytu konfiguracji. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą: a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+,

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

	d. SAML 2,0. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
36	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Realizacja tego wymagania musi opierać się o samo urządzenie – nie dopuszcza się realizacji koncepcji kandydackiej z wykorzystaniem centralnej konsoli zarządzania. Funkcja ta musi być dostępna również w przypadku utraty komunikacji z centralną konsolą zarządzania. Funkcja ta musi być realizowana co najmniej przez graficzny interfejs zarządzania firewallem (GUI).
37	Urządzenie musi zapewniać interfejs API (JSON lub REST lub XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
38	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia.
39	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
40	Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.
41	Wykonawca w ramach postępowania musi dostarczyć wszystkie niezbędne okablowanie konieczne do uruchomienia urządzenia.

2) WYMAGANIA DODATKOWO PUNKTOWANE

Nr	Wymagania dodatkowo punktowane – Integracja z posiadanymi rozwiązaniami bezpieczeństwa 15 PKT
1	Urządzenia muszą być zarządzane z poziomu pojedynczego centralnego systemu zarządzania wraz z posiadanymi przez Zamawiającego rozwiązaniami Palo Alto Networks w zakresie: ➢ Zbieranie i analizowanie logów. ➢ Korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym, b. aplikacjach, c. zagrożeniach d. filtrowaniu stron www. ➢ Tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie 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. ➢ Tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Zamawiający przyzna dodatkowe 15 punktów, jeżeli dostarczony system zarządzania będzie mógł objąć urządzenia bezpieczeństwa będące obecnie w użytkowaniu Zamawiającego.
Nr	**Wymagania dodatkowo punktowane – wartość techniczna 20 PKT**

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

2.	Urządzenie musi posiadać w chwili dostawy zarówno funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji oraz funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem. Obie funkcje muszą być dostarczone wraz z subskrybcjami – o ile takie są wymagane przez producenta firewalli. Szczegółowe wymagania zostały opisane w p.28 i p.29 OPZ. Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt.
3.	System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać 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 powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt.
4.	Urządzenie Firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, 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. Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt.
5.	W przypadku utraty komunikacji z centralną konsolą zarządzania urządzenie musi pozwalać na: ➢ Lokalne zbieranie i analizowanie logów. ➢ Korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym, b. aplikacjach, c. zagrożeniach d. filtrowaniu stron www. ➢ Tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie 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. ➢ Tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Jeżeli urządzenie spełnia wymóg – oferta otrzymuje 5 pkt.
Nr	**Wymagania dodatkowo punktowane – dojrzałość rozwiązania 5 PKT**
6	Zamawiający przyzna dodatkowe 5 punktów, jeśli producent oferowanego rozwiązania w postępowaniu był wskazywany w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części („ćwiartce) Leaders w co najmniej jednym raporcie opublikowanym w ciągu ostatnich 18 miesięcy liczonym od terminu składania ofert.

3) WYMAGANIA GWARANCYJNE I SERWISOWE

1. Wykonawca wraz z dostawą urządzeń przekaże warunki gwarancyjne i serwisowe, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

2. Wymagania gwarancyjne:
   1) Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu:
      a) prawo do pobierania nowych wersji i aktualizacji oprogramowania przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu,
      b) przyjmowanie zgłoszeń Zamawiającego przez Wykonawcę 24 godziny na dobę (dla sprzętu objętego serwisem NBD, zgłoszenia zamawiającego dokonane po godz. 15:35 i w dni wolne od pracy będą traktowane jako zgłoszenia dokonane następnego dnia roboczego),
      c) wymianę sprzętu na sprawny w przypadku zdiagnozowania awarii urządzenia,
      d) dostarczenie sprawnego urządzenia lub jego elementu podlegającego wymianie do miejsca zainstalowania urządzenia uszkodzonego,
      e) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania,
      f) dostęp do pomocy technicznej producenta,
      g) dostęp do poprawek i nowych wersji oprogramowania;
   2) gwarancją producenta muszą zostać objęte wszystkie dostarczone urządzenia przez okres minimum 36 miesięcy, przy czym bieg okresu gwarancji rozpocznie się w dniu następnym po dacie podpisania bez zastrzeżeń protokołu zdawczo-odbiorczego. Do dostarczonych urządzeń będą dołączone karty gwarancyjne zawierające numery seryjne produktu, numery seryjne oprogramowania, termin i warunki ważności gwarancji (zgodnie z umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
3. Do przedmiotu zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie edytowalnych dokumentów w wersji elektronicznej.
5. Wykonawca zobowiązuje się do świadczenia usług gwarancyjnych w trybie NBD (następny dzień roboczy).
6. Ilekroć w treści niniejszego dokumentu jest mowa o awarii rozumie się taki stan sprzętu i oprogramowania, który uniemożliwia korzystanie z dostarczonego sprzętu.
7. Zamawiający wymaga, aby awaria została usunięta następnego dnia roboczego od chwili jej zgłoszenia, dotyczy serwisu NBD.
8. W przypadku braku możliwości wykonania naprawy w terminie podanym wyżej, Wykonawca na okres przedłużającej się naprawy bądź usuwania awarii, dostarczy Zamawiającemu sprzęt zastępczy, równoważny funkcjonalnie. Po zakończeniu naprawy sprzęt zastępczy zostanie zwrócony Wykonawcy z wyłączeniem nośników danych.
9. Uszkodzone elementy sprzętu będą wymienione przez Wykonawcę na nowe, wolne od wad i o parametrach nie gorszych od uszkodzonych.
10. W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez gwaranta na nowy bez konieczności zwrotu uszkodzonego dysku twardego lub innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
11. Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzętu i systemu operacyjnego sprzed wystąpienia awarii.
12. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.
13. Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
14. Dla oprogramowania obowiązują prawa gwarancyjne producenta.
15. Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy Producenta, rozbudowy posiadanych urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl

16. Zamawiający zastrzega sobie prawo do dodawania nowych modułów dowolnych producentów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą.

4) ZASADY OGÓLNE

1. Wykonawca zobowiązany jest wykonać przedmiot zamówienia wraz ze wszystkimi wymaganymi dokumentami nie później niż do dnia 10.12.2021 r.
2. Odbiór przedmiotu Umowy zostanie przeprowadzony w 72-100 Goleniów, Glewice Lotnisko Szczecin Goleniów.
3. Odbiór przedmiotu Umowy zostanie potwierdzony podpisaniem przez wyznaczonych przedstawicieli Zamawiającego i Wykonawcy protokołu zdawczo-odbiorczego.
4. Protokół zostanie sporządzony w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Wszelkie pozostałe kwestie i szczegółowe postanowienia w zakresie realizacji przedmiotu zamówienia regulować będzie umowa zawarta pomiędzy Zamawiającym a Wykonawcą.

LOTNICZE POGOTOWIE RATUNKOWE
ul. Księżycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933,
www.lpr.com.pl