**Załącznik nr 1 do SIWZ wzór Formularza Ofertowego**

**Formularz Ofertowy**

**DPiZP.2610.27.2019**

Ja(my) niżej podpisany(-i) ……………………………………………………………………………………………………………………………………………………….

Działając w imieniu i na rzecz ……………………………………………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………………………………………………………………………………………

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na **„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami*”***, zgodnie z wymaganiami określonymi w specyfikacji istotnych warunków zamówienia i wzorze Umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia za cenę:

**Tabela nr 1A**

**Firewall’e – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla pojedynczego Firewall’a** | Parametry oferowane  (zaznacza Wykonawca) |
| 1 | Firewall musi być dostarczony jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19”.  Całość Sprzętu IT musi być zarządzana przez jednego producenta. | TAK/NIE\* |
| 2 | Firewall musi być wyposażony w:   1. 4 interfejsy 100/1000/10GE Ethernet (RJ45) 2. 16 interfejsów 1/10GE SFP+ (z czego 12 interfejsów obsadzonych modułami 10GE SFP+ SR) 3. 4 interfejsy 40GE/100GE QSFP+ lub alternatywnie 4 interfejsy 40GE QSFP+ i 4 interfejsy 100GE QSFP+ | TAK/NIE\* |
| 3 | Firewall musi być wyposażony w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). | TAK/NIE\* |
| 4 | Firewall musi być wyposażony w dedykowany port konsoli/zarządzania. Port ten musi być wydzielony logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. | TAK/NIE\* |
| 5 | Firewall musi spełniać następujące parametry wydajnościowe, jeżeli Firewall może pracować w różnych trybach to jego wydajność musi być mierzona w trybie pracy, który pozwala na uruchomienie wszystkich wymaganych funkcji Sprzętu IT:   1. minimum 40 Gbps dla Firewall/kontroli aplikacji; 2. minimum 20 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji; 3. minimum 280 tys. nowych połączeń na sekundę; 4. minimum 8 000 000 równoległych sesji. | TAK/NIE\* |
| 6 | Firewall musi umożliwiać działanie w trzech trybach pracy:   1. rutera (tzn. w warstwie 3 modelu OSI); 2. przełącznika (tzn. w warstwie 2 modelu OSI); 3. w trybie pasywnego nasłuchu (sniffer). | TAK/NIE\* |
| 7 | Tryb pracy Firewall-a 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 (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.). | TAK/NIE\* |
| 8 | * + - 1. Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN.       2. Firewall musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q.       3. Firewall musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3. | TAK/NIE\* |
| 9 | * + - 1. Firewall musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną.       2. 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. | TAK/NIE\* |
| 10 | * 1. Firewall musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.   2. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN).   3. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN | TAK/NIE\* |
| 11 | * + - 1. Firewall musi spełniać następujące parametry wydajnościowe:   1. minimum 15Gbps **przepustowości dla ruchu IPSec**   2. minimum **5 000** tuneli IPSEC VPN (site-to-site)   3. minimum **10 000** tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.      + 1. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji lub jeżeli dedykowany klient VPN (dla systemów: Windows, Linux, Android, MacOS) oferowany przez producenta Sprzętu IT wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla **3 000** jednoczesnych użytkowników. | TAK/NIE\* |
| 12 | Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach:   1. Polityki definiujące powinny umożliwiać wykorzystanie:    * 1. adresów źródłowych      2. adresów docelowych      3. użytkowników      4. numerów portów usług      5. kategorie URL 2. System musi obsługiwać następujące mechanizmy uwierzytelnienia    * 1. RADIUS lub TACACS+      2. LDAP      3. Kerberos lub SAML 2.0 | TAK/NIE\* |
| 13 | Firewall musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie:   1. oznaczania pakietów znacznikami DiffServ; 2. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego; 3. utworzenia 8 klas ruchu sieciowego; 4. kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników; 5. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP; 6. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. | TAK/NIE\* |
| 14 | Firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP | TAK/NIE\* |
| 15 | Firewall musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP. | TAK/NIE\* |
| 16 | * + - 1. Firewall musi obsługiwać nie mniej niż 50 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.       2. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych). | TAK/NIE\* |
| 17 | Firewall musi obsługiwać nie mniej niż 25 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 75 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:   * 1. tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych);   2. Polityk bezpieczeństwa obejmujących:      1. System IPS;      2. System ochrony antymalware/antyspyware;      3. System ochrony antywirus;   3. Koncentratorów VPN dla zdalnego dostępu. | TAK/NIE\* |
| 18 | Firewall musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu. | TAK/NIE\* |
| 19 | * + - 1. Firewall musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie firewall-i.       2. Firewall-e w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active. | TAK/NIE\* |
| 20 | 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.  Firewall musi umożliwiać zdefiniowanie nie mniej niż 50 000 reguł polityki bezpieczeństwa. | TAK/NIE\* |
| 21 | * + - 1. Identyfikacja aplikacji musi odbywać się poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji Sprzętu IT numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji.       2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.       3. Firewall musi wykrywać 2500 predefiniowanych aplikacji wspieranych przez producenta (w szczególności: 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 Sprzęcie IT bez użycia zewnętrznych narzędzi. | TAK/NIE\* |
| 22 | Firewall musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa.  W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość” w polityce. | TAK/NIE\* |
| 23 | * + - 1. Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja.       2. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. | TAK/NIE\* |
| 24 | Firewall 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. | TAK/NIE\* |
| 25 | Firewall 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. | TAK/NIE\* |
| 26 | Firewall musi zapewniać ochronę przed atakami typu „Drive-by-download”. | TAK/NIE\* |
| 27 | * + - 1. Firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.       2. Wymagana jest obsługa deszyfracji i inspekcji protokołu HTTP/2 zarówno dla ruchu inbound jak i outbound. | TAK/NIE\* |
| 28 | Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH | TAK/NIE\* |
| 29 | Firewall musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:   1. Microsoft Active Directory; 2. usługi katalogowe LDAP; 3. serwery Terminal Services. | TAK/NIE\* |
| 30 | Polityka kontroli dostępu Firewall-a 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. | TAK/NIE\* |
| 31 | Firewall musi posiadać możliwość 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.  Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.  Dopuszcza się zastosowanie innego mechanizmu wbudowanego w Firewall który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia” logowania użytkowników. | TAK/NIE\* |
| 32 | * + - * 1. Firewall musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji.         2. System IPS musi działać w warstwie 7 modelu OSI.         3. Baza sygnatur IPS/IDS musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent Sprzętu IT.         4. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).         5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi. | TAK/NIE\* |
| 33 | Firewall musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji.  Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder, w szczególności: http, smtp, imap, pop3, ftp, smb.  Baza sygnatur AV musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń  Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall.  Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). | TAK/NIE\* |
| 34 | Firewall musi zapewniać ochronę przed atakami typu Spyware – dopuszcza się 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 Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.  Reguły/silnik anty-spyware musi być uruchamiany per reguła polityki bezpieczeństwa firewall.  Nie jest dopuszczalne, aby funkcja ta była uruchamiana per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi i wsparcia producenta.  Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania. | TAK/NIE\* |
| 35 | Firewall 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). | TAK/NIE\* |
| 36 | Firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. | TAK/NIE\* |
| 37 | Firewall musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji.  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 cały Firewall 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.  Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania. | TAK/NIE\* |
| 38 | * + - 1. Firewall musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.       2. Firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day.       3. 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. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to nie wymagane jest jej dostarczenie w chwili zakupu Firewalla/i. | TAK/NIE\* |
| 39 | Zarządzanie Firewall-em musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę www.  Dostęp do Firewall-a i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). | TAK/NIE\* |
| 40 | * + - 1. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.       2. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą:  1. bazy lokalnej; 2. serwera LDAP; 3. RADIUS lub TACACS+.    * + 1. Firewall musi zapewniać tworzenie sekwencji uwierzytelniającej posiadającej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). | TAK/NIE\* |
| 41 | Firewall musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu Firewall-a bez użycia systemu zarządzania lub linii poleceń (CLI). | TAK/NIE\* |
| 42 | Firewall musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym Firewall-a. | TAK/NIE\* |
| 43 | Firewall musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych. | TAK/NIE\* |
| 44 | Firewall musi umożliwiać bieżące wysyłanie logów do zewnętrznych serwerów SYSLOG oraz posiadać możliwość wysyłania logów z wykorzystaniem protokołu TCP i zdefiniowana portu docelowego. | TAK/NIE\* |
| 45 | Firewall musi być wyposażony w zasilacze typu AC pracujące redundantnie. | TAK/NIE\* |

**Uwaga 1**

**\*-niewłaściwe przekreślić***.*

**Tabela nr 1B**

**System zarządzania:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla systemu zarządzania** | Parametry oferowane  (zaznacza Wykonawca) |
| 1 | Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania.  Dopuszcza się budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta Firewall-i i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane.  System zarządzania musi pracować w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów. | TAK/NIE\*\* |
| 2 | System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMWare. | TAK/NIE\*\* |
| 3 | System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne:   1. obsługa nie mniej niż 10 firewalli fizycznych 2. obsługa nie mniej niż 10 firewalli wirtualnych 3. zapewnienie obsługi przestrzeni dyskowej o pojemności nie mniejszej niż 10 TB. 4. Możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczonej na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji) | TAK/NIE\*\* |
| 4 | 1. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach www. 2. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli | TAK/NIE\*\* |
| 5 | System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym:   1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 2. tworzenie statycznych raportów dopasowanych do wymagań Kupującego. 3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 4. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Kupującego z funkcjonalnością „drill-down”. | TAK/NIE\*\* |
| 6 | System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym:   1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. 2. lokalnych (dla wybranych firewalli lub logicznych systemów firewalla). 3. globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). 4. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów) 5. pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń. 6. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. 7. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 8. umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi. | TAK/NIE\*\* |
| 7 | System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym musi:   1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu; 2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli; 3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur; 4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem; 5. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów; 6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone; 7. informować o zmianach konfiguracji systemu. | TAK/NIE\*\* |
| 8 | System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów. | TAK/NIE\*\* |

**Uwaga 2**

**\*\*-niewłaściwe przekreślić**

**TABELA nr 2 – Wymagania dodatkowe punktowane w ramach kryterium „Parametry techniczne Sprzętu IT”**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **„Parametry techniczne Sprzętu IT” (PT)** | **Parametr oferowany zaznacza Wykonawca** |
| 1. | Automatycznie identyfikuje aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną | TAK/NIE**\*\*\*** |
|  | Blokuje transmisję plików szyfrowanych co najmniej:   * 1. Dokumentów office (doc, xls, ppt, docx, xlsx, pptx)   2. Plików skompresowanych (zip, rar) | TAK/NIE **\*\*\*** |
|  | Wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym/fizycznym | TAK/NIE **\*\*\*** |
|  | Posiada koncept konfiguracji kandydackiej którą można dowolnie edytować na Firewall-u bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji Firewall-a do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym:   1. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. 2. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji | TAK/NIE **\*\*\*** |
|  | Sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem do użycia) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w Firewall-a i nie może wymagać korzystania z rozwiązań trzecich | TAK/NIE **\*\*\*** |
|  | W przypadku utraty komunikacji z centralnym systemem zarządzania Firewall musi pozwalać na:   1. Lokalne konfigurowanie reguł bezpieczeństwa 2. Lokalne zbieranie i analizowanie logów 3. korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:    1. ruchu sieciowym    2. aplikacjach    3. zagrożeniach    4. filtrowaniu stron www 4. 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 5. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu | TAK/NIE **\*\*\*** |
|  | System zarządzania, logowania i raportowania posiada taki sam graficzny Interfejs Użytkownika (GUI) jak zarządzane Firewall-e | TAK/NIE **\*\*\*** |
|  | System zarządzania, logowania i raportowania Firewall-ami umożliwia dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek | TAK/NIE **\*\*\*** |
|  | System zarządzania, logowania i raportowania Firewall-i umożliwia zarządzanie posiadanymi przez Zamawiającego urządzeniami Palo Alto Networks PA-5060 w całościowym zakresie opisanym w wymaganiach dla tego systemu | TAK/NIE **\*\*\*** |

**Uwaga 3:**

*\*\*\*-* **niewłaściwe przekreślić.** *W przypadku nie przekreślenia żadnego ze zwrotów lub łącznego przekreślenia obu zwrotów „TAK/NIE” przez Wykonawcę dla danej pozycji, Zamawiający uzna że zaoferowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.*

**TABELA nr 3**

**Oferujemy Sprzęt IT** o parametrach technicznych wymienionych w Tabeli nr 1A i nr 1B oraz w Tabeli nr 2 (punktowane w ramach kryteriów oceny ofert\*\*\*\*), oraz na warunkach określonych we wzorze Umowy, który stanowi Załącznik nr 6 do SIWZ**za cenę:**

*Uwagi:*

*\*\*\*\* - o ile są oferowane*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Przedmiot** | **Cena ofertowa netto zł** | **Podatek VAT** | | **Cena ofertowa brutto zł** |
| **%** | **zł** |
| **a** | **b** | **c** | **d = b x c** | **e = b + d** |
| 1. | Sprzęt IT (Firewall - 2 szt. wraz z systemem zarządzania) oraz z Oprogramowaniem, spełniający wymagania określone w Tabeli nr 1A, nr 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym przez 36 miesięcy wg wymagań zdefiniowanych w § 6 wzoru umowy.  ***Producent***  ***……………………….***  ***Model Firewall***  ***……………………….*** |  |  |  |  |
| 2. | Wdrożenie i Dokumentacja powykonawcza, zgodnie z  § 7 ust. 1 pkt. 2) wzoru Umowy |  |  |  |  |
| **Razem [∑1÷2]:** | |  | **X** |  |  |

**Tabela nr 4**

| **Lp.** | **Przedmiot zamówienia** | **Ilość**  **jednostek** | **Cena jednostkowa netto (zł)**  *(cena za 1 godz. konsultacji)* | **Cena ofertowa netto (zł)** | **Podatek**  **VAT** | | **Cena ofertowa brutto (zł)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **%** | **zł** |
| *[a]* | *[b]* | *[c]* | *[d]* | *[e] = [c] x [d]* | *[f]* | *[g] = [e] x [f]* | *[h] = [e] + [g]* |
| **1** | Konsultacje, o których mowa w § 2 ust. 4 i 5 wzoru Umowy | **500 godz.** |  |  |  |  |  |

**Tabela nr 5 - Łączna cena oferty**

| **Przedmiot** | | **Cena netto**  **[zł]** | **Podatek VAT**  **[zł]** | **Cena brutto**  **[zł]** |
| --- | --- | --- | --- | --- |
| *[a]* | *[b]* | *[c]* | *[d]* | *[e]* |
| 1 | Sprzęt IT (Firewall - 2 szt. wraz z systemem zarządzania) oraz z Oprogramowaniem, spełniający wymagania określone w Tabeli nr 1A, nr 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym przez 36 miesięcy wg wymagań zdefiniowanych w § 6 wzoru Umowy  oraz  Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru umowy, **- wg Tabeli nr 3**  *(należy wpisać odpowiednio wartości z Tabeli nr 3 z pozycji „Razem”:*  *kol. „b”, „d” i „e”)* |  |  |  |
| 2 | Konsultacje, o których mowa w § 2 ust. 4 i 5 wzoru Umowy **– wg Tabeli nr 4**  *(należy wpisać odpowiednio wartości z Tabeli nr 4:*  *kol. „e”, „g” i „h”)* |  |  |  |
| **Łączna cena oferty [∑1÷2]:** | |  |  |  |

**Łączna cena netto oferty ………………………. zł słownie:**

**Łączna cena brutto oferty ………………………. zł słownie:**

**Oświadczamy, że:**

1. **Termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy wyniesie…….. Dni Roboczych.**
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdziale II SIWZ oraz wzorze Umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Zapoznaliśmy się z treścią SIWZ (w tym ze wzorem Umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
5. Uważamy się za związanych niniejszą ofertą na okres wskazany w SIWZ.
6. Wadium w wysokości **19 000,00 zł** (słownie: dziewiętnaście tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
7. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr …………………………………………………………………………………………….………prowadzony w banku ………….………….
8. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **10%** ceny całkowitej podanej w ofercie.
9. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu  i terminie wskazanym przez Zamawiającego.
10. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz firmę Podwykonawcy):
11. ………………………………………………………………………………………………………………………………………………………………………………………………………………………………………\*

\* *w* przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*

1. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres: ………………………………………………………………………………………………………………   
   Dane kontaktowe: imię i nazwisko ……………………………………………………………, nr tel. ……………………………………………….., adres e-mail: ……………………………………………………..
2. Dokumenty wymienione od strony ……… do strony ……… stanowią tajemnicę przedsiębiorstwa i nie mogą być ujawnione pozostałym uczestnikom postępowania.

***UWAGA****:*

*Zamawiający przypomina, że stosownie do art. 8 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.*

1. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)\*wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*\*

*\* rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1* oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.*).*

*\*\* w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*

1. Jednocześnie zgodnie z treścią art. 91 ust. 3a ustawy oświadczam, że wybór przedmiotowej oferty:\*
   * 1. **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego
     2. **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług

------------------------------------------------------------------------------------------------------------------------------------------

*(należy wskazać: nazwę (rodzaj) towarów/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz wartość bez kwoty podatku od towarów i usług)*

\*) Niepotrzebne skreślić. W przypadku nie skreślenia (nie wskazania) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: *„należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług”* – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

1. Oferta została złożona na \_\_\_\_\_\_ stronach kolejno ponumerowanych od nr\_\_\_\_\_\_\_ do nr \_\_\_\_\_\_\_.

*Świadom odpowiedzialności karnej oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień złożenia oferty (art. 297 k.k.).*