**Załącznik nr 2 do SWZ**

 **Postępowanie nr 368/2023/PN/DZP**

**FORMULARZ OPIS PRZEDMIOTU ZAMÓWIENIA/FORMULARZ CENOWY**

**Opis oferowanego sprzętu.**

Uwagi dot. Tabeli:

Wykonawca wpisuje odpowiednio:

1. W tabeli zawarte są wybrane informacje istotne dla Zamawiającego (Wykonawca w swojej ofercie może uwzględnić inne, nie wymienione tutaj elementy, niezbędne do realizacji wymagań Zamawiającego, które nie muszą być wykazane w tabeli).
2. Gdy w polu „Nazwa parametru” występuje słowo „Producent” lub „Model”, proszę w polu „Opis/Wartość” wpisać nazwę producenta oraz model oferowanego urządzenia.
3. Jeżeli w polu „Nazwa parametru” występuje podpowiedź „[szt.]” proszę w polu „Opis/Wartość” wpisać odpowiednią wartość liczbową.
4. Jeżeli w polu „Nazwa parametru” występuje podpowiedź „[Tak/Nie]” proszę w polu „Opis/Wartość” wpisać słowo „Tak” lub „Nie” w odpowiedzi na zadane pytanie.
5. Jeżeli w polu „Nazwa parametru” występuje podpowiedź „[Gbps]” proszę w polu „Opis/Wartość” wpisać liczbę Giga bitów na sekundę (1Gbps = 109 bitów na sekundę)
6. Jeżeli w polu „Nazwa parametru” występuje podpowiedź „[GB]” proszę w polu „Opis/Wartość” wpisać liczbę Gigabajtów (1GB = 230 lub 1 073 741 824 bajtów)
7. Jeżeli w polu „Opis/Wartość” występuję „N/d” „(Nie dotyczy)” oznacza to początek zaznaczonej wcięciem grupy parametrów.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **lp.** | **Typ****urządzenia** | **Nazwa parametru** | **Opis/Wartość** |  **Cena brutto** |
|  **1.** | **Komponent Zabezpieczający**(parametry techniczne dotyczą pojedynczego urządzenia) | Producent |  |  |
| Model |  |
| Liczba dostarczanych urządzeń [szt.] |  |
| Liczba Zasilaczy [szt.] |  |
|  | Czy zasilacze mają możliwość wymiany w trybie hot-swap [Tak/Nie] |  |
| Czy awaria połowy zasilaczy zainstalowanych w urządzeniu ma jakikolwiek wpływ na działanie urządzenia [Tak/Nie] |  |
| Ilość faz 230V/50Hz wymaganych do zasilenia urządzenia [szt.] |  |
| Czy System pozwala na import reguł zgodnych z rozwiązaniami SNORT i/lub Suricata do modułów systemu wykrywania i zapobiegania włamaniom komponentu zabezpieczającego [Tak/Nie] |  |
| Interfejsy (jeżeli urządzenie posiada jeszcze inne niż wymienione poniżej to proszę je podać) | N/d |
|  | Ilość interfejsów o przepustowości minimum 10 Gbps typu SFP+ zakończonych wkładkami światłowodowymi o zasięgu transmisji nie mniejszym niż 10 km [szt.] |  |
| Ilość interfejsów o przepustowości minimum 10 Gbps typu RJ45 [szt.] |  |
| Ilość interfejsów o przepustowości minimum 100 Gbps zakończonych wkładkami światłowodowymi o zasięgu transmisji nie mniejszym niż 10 km [szt.] |  |
| Pojemność przestrzeni dyskowej działającej w konfiguracji RAID-1, przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi) [GB] |  |
| Parametry wydajnościowe | N/d |
|  | Przepustowości (ang. throughput) dla ruchu rzeczywistego z włączoną kontrolą aplikacji, włączonym logowaniem |  |
| Przepustowości (ang. throughput) dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (Firewall, IPS, antywirus, anty-spyware, współpraca z sandboxem, kontrola aplikacji, włączone logowanie), |  |
| Liczba nowych połączeń na sekundę [szt.] |  |
| Liczba równoległych sesji [szt.] |  |
| Przepustowość (ang. throughput) dla IPSEC VPN [Gbps] |  |
| Liczba tuneli tuneli IPSEC VPN (site-to-site) [szt.] |  |
| Czy komponent zabezpieczający ma możliwość pracy w trybie routera (tzn. w warstwie 3 modelu ISO OSI) [Tak/Nie] |  |
| Czy komponent zabezpieczający ma możliwość pracy w trybie przełącznika (tzn. w warstwie 2 modelu ISO OSI) [Tak/Nie] |  |
| Liczba znaczników VLAN zgodnych z 802.1q obsługiwanych przez interfejsy sieciowe pracujące w standardzie Ethernet [szt.] |  |
| Czy komponent zabezpieczający umożliwia translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. [Tak/Nie] |  |
| Parametry związane z QOS | N/d |
|  | Czy komponent zabezpieczający ma możliwość oznaczania pakietów znacznikami DiffServ [Tak/Nie] |  |
| Czy komponent zabezpieczający ma możliwość ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego [Tak/Nie] |  |
| Czy komponent zabezpieczający ma możliwość utworzenia co najmniej 8 klas ruchu sieciowego [Tak/Nie] |  |
| Czy komponent zabezpieczający realizuje funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia obsługę protokołów routingu minimum OSPF w wersji 2 i 3, BGP, wraz z BFD [Tak/Nie] |  |
| Czy komponent zabezpieczający obsługuje nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu. [Tak/Nie] |  |
| Czy dostarczony komponent zabezpieczający będzie obsługiwał nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów [Tak/Nie] |  |
| Czy komponent zabezpieczający posiada możliwość rozbudowy do co najmniej 20 wirtualnych firewalli/systemów/domen/kontekstów [Tak/Nie] |  |
|   | N/d |
|  | tablic routingu [Tak/Nie] |  |
| polityk bezpieczeństwa obejmujących system IPS [Tak/Nie] |  |
| polityk bezpieczeństwa obejmujących system ochrony antymalware/antyspyware [Tak/Nie] |  |
| polityk bezpieczeństwa obejmujących system ochrony antywirus [Tak/Nie] |  |
| polityk bezpieczeństwa obejmujących tunele VPN IPSec [Tak/Nie] |  |
| Czy komponent zabezpieczający wspiera mechanizm PBR (policy based routing) [Tak/Nie] |  |
| Czy polityka bezpieczeństwa komponentu zabezpieczającego prowadzi kontrolę ruchu sieciowego i uwzględnia strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. [Tak/Nie] |  |
| Ilość możliwych do zdefiniowania reguł polityki bezpieczeństwa [szt.] |  |
| Ilość możliwych do zdefiniowania stref bezpieczeństwa [szt.] |  |
| Czy komponent zabezpieczający umożliwia rozpoznawanie aplikacji bez względu na numery portów, na których działa aplikacja (ang. application/services). [Tak/Nie] |  |
| Czy komponent zabezpieczający wykrywa predefiniowane aplikacje wspierane przez producenta (np. Skype, Tor, BitTorrent, eMule) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS [Tak/Nie] |  |
| Czy komponent zabezpieczający pozwala na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu lub z wykorzystaniem komponentu zarządczego [Tak/Nie] |  |
| Czy komponent zabezpieczający posiada i będzie dostarczony z funkcjonalnością systemu wykrywania i zapobiegania włamaniom (Intrusion Prevention System – IPS) oraz czy baza sygnatur systemu IPS jest przechowywana na urządzeniu [Tak/Nie] |  |
| Czy komponent zabezpieczający posiada i będzie dostarczony z funkcjonalnością systemu Antywirus (AV) oraz czy baza sygnatur systemu AV jest przechowywana na urządzeniu [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewnia ochronę przed atakami typu Spyware oraz czy baza sygnatur systemu Spyware jest przechowywana na urządzeniu [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewnia możliwość wysłania plików do sandboxa producenta [Tak/Nie] |  |
| Czy zarządzanie komponentem zabezpieczającym (w tym zarządzanie regułami/politykami bezpieczeństwa ) odbywa się z linii poleceń (CLI) i graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW [Tak/Nie] |  |
| Czy komponent zabezpieczający pozwala na zdefiniowanie wielu administratorów o różnych uprawnieniach [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia uwierzytelnianie administratorów za pomocą co najmniej dwóch z następujących metod: baza lokalna, LDAP, RADIUS lub TACACS+ [Tak/Nie] |  |
| Czy praca na urządzeniu będącym komponentem zabezpieczającym odbywa się na konfiguracji tymczasowej, a nie aktywnej oraz czy istnieje możliwość przejrzenia zmian przed ich zatwierdzaniem na urządzeniu [Tak/Nie] |  |
| Ilość poprzednich wersji konfiguracji możliwych do zapisania w przestrzeni dyskowej urządzenia będącego komponentem zabezpieczającym [szt.] |  |
| Czy istnieje możliwość przywrócenia konfiguracji komponentu zabezpieczającego z dowolnej, zapisanej uprzednio na dysku konfiguracji [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewnia interfejs API (JSON, REST, XML lub inny) będący integralną częścią urządzenia, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI) [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia eksportowanie logów do zewnętrznych serwerów SYSLOG z wyłączeniem serwerów pośredniczących [Tak/Nie] |  |
| Przepustowość dla inspekcji ruchu SSL/TLS (ang. SSL Inspection Throughput) osiągana przez komponent zabezpieczający lub element dodatkowy [Gbps] |  |
| Czy funkcjonalność inspekcji SSL/TLS jest dostępna w każdej z 20 potencjalnie możliwych do skonfigurowania wirtualnych instancji komponentu zarządzającego [Tak/Nie] |  |
| Wymagania odnośnie elementu dodatkowego dostarczanego w celu spełnienia wymaganych funkcjonalności komponentu zabezpieczającego (z wyjątkiem funkcji wykrywania aplikacji, obsługi IPS, AV i NAT) | N/d(Jeżeli żaden element dodatkowy nie jest wymagany proszę wpisać poniżej „N/d”) |
|  | Czy wspomniany powyżej element dodatkowy jest serwisowany w całości przez jednego producenta), oraz czy posiada pełną redundnacją sprzętową i spełnienia wymagania dotyczące zasilania urządzenia analogicznie jak dla urządzeń Next Generation Firewall (NGFW) [Tak/Nie] |  |
| Czy element dodatkowy spełnia wymagania zdefiniowane dla całego Systemu [Tak/Nie] |  |
| Czy urządzenia realizujące funkcję inspekcji SSL/TLS, są połączone z urządzeniami Next Generation Firewall (NGFW) za pomocą co najmniej 8 interfejsów 10 Gbps i wkładkami o przepustowości 10 Gbps (transmisja na odległość min. 10km) [Tak/Nie]  |  |
| Czy element dodatkowy ma możliwość wysyłania zdarzeń do zewnętrznych serwerów SYSLOG. [Tak/Nie] |  |
| Wymagania na realizację funkcjonalności zdalnych sesji VPN (ang. remote access VPN) dla użytkowników  | N/d |
|  | Czy komponent zabezpieczający obsługuje funkcjonalność zdalnych sesji VPN umożliwiającą realizację zdalnych sesji VPN przez użytkowników z wykorzystaniem aplikacji klienckich instalowanych na stacjach roboczych (ang. desktop clients) [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewnia realizację co najmniej 3000 jednoczesnych zdalnych sesji VPN. [Tak/Nie]  |  |
| Czy komponent zabezpieczający umożliwia zestawianie tuneli SSL VPN z wykorzystaniem klienta VPN dostarczonego przez producenta urządzenia NGFW dla co najmniej 3000 użytkowników. [Tak/Nie] |  |
| Czy wykorzystanie funkcjonalności zdalnych sesji VPN zgodnie z wymaganiami Zamawiającego wymaga zakupu dodatkowych licencji? Jeżeli tak to czy są już uwzględnione w ofercie Wykonawcy [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia obsługę zdalnych sesji VPN z wykorzystaniem protokołu IPSec (ang. Internet Protocol Security) oraz protokołu SSL (ang. Secure Sockets Layer) co najmniej dla dostępu z wykorzystaniem aplikacji klienckich instalowanych na stacjach roboczych [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia tunelowanie całego ruchu pochodzącego od stacji klienckiej z wykorzystaniem połączenia VPN oraz tunelowanie jedynie ruchu kierowanego do wybranych adresów IP tzw. dzielone tunelowanie VPN (ang. split-tunneling) [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewnia konfigurowanie polityk dostępu umożliwiających dostęp do określonych zasobów wskazywanych w postaci adresów IP i portów UDP/TCP dla zdalnych sesji VPN [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewnia konfigurowanie polityk połączenia określających co najmniej statyczne pule adresów IP, z których przyznawane są użytkownikom adresy podczas nawiązywania połączenia oraz możliwość wskazywania adresu serwera DNS [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia zakończenie (przerwanie) przez administratora aktywnych zdalnych sesji VPN [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia uzyskanie przez administratora informacji o liczbie aktualnie zalogowanych użytkowników (aktywnych zdalnych sesji VPN) [Tak/Nie] |  |
| Czy aplikacje klienckie umożliwiają realizację połączeń VPN z urządzeń pracujących pod kontrolą co najmniej następujących systemów operacyjnych: Windows 10/11, macOS [Tak/Nie] |  |
| Czy komponent zabezpieczający umożliwia uwierzytelnianie użytkowników zdalnych sesji VPN z wykorzystaniem kont lokalnych oraz z wykorzystaniem co najmniej protokołu LDAP poprzez odwołanie się do zewnętrznego serwera [Tak/Nie] |  |
| Czy przy uwierzytelnianiu użytkowników zdalnych sesji VPN z wykorzystaniem protokołu LDAP istnieje możliwość przypisania dla użytkownika dostępu do określonych zasobów (polityk dostępu) w oparciu o przynależność do grup LDAP do których użytkownik jest przypisany na serwerze LDAP [Tak/Nie] |  |
| Czy komponent zabezpieczający zapewniać logowanie danych dotyczących połączeń zdalnych sesji VPN w zakresie co najmniej: | N/d |
|  | nazwy lub identyfikatora użytkownika nawiązującego połączenie [Tak/Nie] |  |
| adresu IP, z którego nawiązywane jest przez użytkownika połączenie [Tak/Nie] |  |
| daty i godziny nawiązania i zakończenia połączenia [Tak/Nie] |  |
| informacji o zakończonych niepowodzeniem próbach nawiązania sesji przez użytkownika (np. nieprawidłowa autoryzacja) [Tak/Nie] |  |
| przyznanego na czas trwania sesji adresu IP (w przypadku połączenia z wykorzystaniem aplikacji klienta) [Tak/Nie] |  |
| **2.** | **Komponent Zarządczy** | Czy komponent zarządczy pochodzi od tego samego producenta, co urządzenia NGFW wchodzące w skład komponentu zabezpieczającego [Tak/Nie] |  |
| Czy komponent zarządczy umożliwia centralne zarządzanie urządzeniami wchodzącymi w skład komponentu zabezpieczającego (w tym zarządzanie regułami/politykami bezpieczeństwa) przy pomocy graficznej konsoli WebGUI dostępnej przez przeglądarkę WWW [Tak/Nie] |  |
| Czy komponent zarządczy umożliwia zarządzanie wszystkimi urządzeniami NGFW wchodzącymi w skład komponentu zabezpieczającego [Tak/Nie] |  |
| Czy komponent zarządczy będzie umożliwiał zarządzanie łącznie co najmniej 10 fizycznymi urządzeniami NGFW i co najmniej 40 firewallami wirtualnymi rozumianymi jako wirtualny firewalli/system/domena/kontekst [Tak/Nie] |  |
| Jeżeli Wykonawca zastąpi WebGUI innym rozwiązaniem to czy zapewnia ono: | N/d(Jeżeli Wykonawca nie zastępuje WebGUI to proszę wpisać poniżej „N/d”) |
|  | działanie w trybie wysokiej dostępności HA (w celu wykluczenia pojedynczego punktu awarii) [Tak/Nie]  |  |
| wszystkie nieodwoływalne i niezbędne do działania licencje i komponenty [Tak/Nie] |  |
| dostęp dla co najmniej 10 osób jednocześnie [Tak/Nie] |  |
| gwarancję i wsparcie na cały okres gwarancyjny komponentu zabezpieczającego [Tak/Nie] |  |
| Czy komponent zarządczy umożliwia zdefiniowanie co najmniej 10 lokalnych kont administracyjnych z możliwością określenia praw dostępu [Tak/Nie] |  |
| Czy komponent zarządczy umożliwia zarządzanie obiektami używanymi przez wszystkie komponenty zabezpieczające w jednym, centralnym repozytorium [Tak/Nie] |  |
| Czy komponent zarządczy umożliwia dystrybucję i zdalną instalację nowych sygnatur oraz wersji oprogramowania systemowego [Tak/Nie] |  |
| Czy komponent zarządczy jest w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami [Tak/Nie] |  |
| Czy graficzny interfejs (WebGUI) komponentu zarządczego jest dostępny za pomocą protokołu HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii java czy flash [Tak/Nie] |  |
| Czy komponent zarządczy pozwala na obsługę co najmniej 50 logów na sekundę w przypadku logów użytkowników [Tak/Nie] |  |
| Czy komponent zarządczy pozwala na przyrost dzienny logów użytkowników na poziomie nie mniejszym niż 1,5 GB [Tak/Nie] |  |
| Czy komponent zarządczy umożliwia retencję danych nie krótszą niż 5 lat w przypadku logów administracyjnych [Tak/Nie] |  |
|  **Łącznie wartość brutto (w tym 0% stawki podatku VAT)** |  |

Oświadczamy, że:

1. zamówienie zostanie zrealizowane w zadeklarowanym terminie;
2. w cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia;
3. zapoznaliśmy się ze Specyfikacją Warunków Zamówienia oraz stanowiącymi jej integralną część załącznikami i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte;