**Znak sprawy: ZP.382.20.2022**

**Załącznik nr 5 do SWZ**

**ZADANIE NR 3**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostawa klastra urządzeń klasy UTM wraz z subskrypcją zabezpieczeń**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | | **Opis minimalnych wymaganych parametrów technicznych** | **Wartość wymagana** | **Parametr/ Wartość oferowana** |
| **Wymagania ogólne** | | |  |  |
| **1.** | | Sprzęt fabrycznie nowy, niepowystawowy | TAK |  |
| **2.** | | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT, transparentnym. | TAK |  |
| **3.** | | W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 2 administratorów do poszczególnych instancji systemu. | TAK |  |
| **4.** | | Komplet urządzeń musi zostać dostarczony i skonfigurowany według zaleceń zamawiającego. |  |  |
| **5.** | | System musi wspierać IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. | TAK |  |
| **SYSTEM BEZPIECZEŃSTWA – UTM:** | | |  | **Model, nazwa /nr katalogowy ……………………………….**  **Producent ……………………………………..……………….**  **Kraj pochodzenia …………………………….….……………**  **Rok produkcji …………………………………………………** |
| **Redundancja, monitoring i wykrywanie awarii:** | | |  |  |
| 6. | | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Passive | TAK |  |
| 7. | | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. | TAK |  |
| 8. | | Monitoring stanu realizowanych połączeń VPN. | TAK |  |
| 9. | | System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. | TAK |  |
| **Interfejsy, Dysk, Zasilanie:** | | |  |  |
| 10. | | System realizujący funkcję Firewall musi dysponować minimum:  • 8 portami Gigabit Ethernet RJ-45. | TAK |  |
| 11. | | System Firewall musi posiadać gniazdo USB umożliwiające podłączenie modemu 3G/4G | TAK |  |
| 12. | | W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych -definiowanych jako VLAN’y w oparciu o standard 802.1Q. | TAK |  |
| 13. | | System musi być wyposażony w zasilanie AC. | TAK |  |
| **Parametry wydajnościowe:** | | |  |  |
| 14. | | W zakresie Firewall’a obsługa nie mniej niż 4 mln. jednoczesnych połączeń | TAK |  |
| 15. | | Przepustowość Stateful Firewall: nie mniej niż 15 Gbps | TAK |  |
| 16. | | Ilość nowych połączeń na sekundę: nie mniej niż 90 tys. | TAK |  |
| 17. | | Wydajność szyfrowania IPSec VPN nie mniej niż 1,5 Gbps. | TAK |  |
| 18. | | Wydajność skanowania ruchu z włączoną funkcją IPS - minimum 2,5 Gbps. | TAK |  |
| 19. | | Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. | TAK |  |
| 20. | | Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. | TAK |  |
| **Funkcje Systemu Bezpieczeństwa:**  **W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:** | | |  |  |
| 21. | | Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. | TAK |  |
| 22. | | Kontrola Aplikacji. | TAK |  |
| 23. | | Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. | TAK |  |
| 24. | | Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. | TAK |  |
| 25. | | Ochrona przed atakami - Intrusion Prevention System. | TAK |  |
| 26. | | Kontrola stron WWW. | TAK |  |
| 27. | | Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. | TAK |  |
| 28. | | Zarządzanie pasmem (QoS, Traffic shaping). | TAK |  |
| 29. | | Funkcja scentralizowanego przechowywania logów | TAK |  |
| 30. | | Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. | TAK |  |
| 31. | | Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. | TAK |  |
| 32. | | Analiza ruchu szyfrowanego protokołem SSH. | TAK |  |
| 33. | | Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system | TAK |  |
| **Polityki, Firewall** | | |  |  |
| 34. | | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. | TAK |  |
| 35. | | System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  • Translację jeden do jeden oraz jeden do wielu.  • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. | TAK |  |
| 36. | | W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa przynajmniej DMZ, LAN, WAN. | TAK |  |
| 37. | | Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. | TAK |  |
| **Połączenia VPN** | | |  |  |
| 38. | | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  • Wsparcie dla IKE v1 oraz v2.  • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.  • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.  • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu oraz routingu statycznego.  • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.  • Mechanizm „Split tunneling” dla połączeń Client-to-Site. | TAK |  |
| 39. | | System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.  • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.  • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.  Routing i obsługa łączy WAN  1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  • Routingu statycznego.  • Policy Based Routingu.  • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. | TAK |  |
| **Funkcje SD-WAN** | | |  |  |
| 40. | | System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. | TAK |  |
| 41. | | Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. | TAK |  |
| **Zarządzanie pasmem** | | |  |  |
| 42. | | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | TAK |  |
| 43. | | Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. | TAK |  |
| 44. | | System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | TAK |  |
| **Ochrona przed malware** | | |  |  |
| 45. | | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach | TAK |  |
| 46. | | System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. | TAK |  |
| 47. | | System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). | TAK |  |
| 48. | | System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. | TAK |  |
| 49. | | System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. | TAK |  |
| 50. | | Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | TAK |  |
| **Ochrona przed atakami:** | | |  |  |
| 51. | | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. | TAK |  |
| 52. | | System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. | TAK |  |
| 53. | | Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora | TAK |  |
| 54. | | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. | TAK |  |
| 55. | | System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS | TAK |  |
| 56. | | Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. | TAK |  |
| 57. | | Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | TAK |  |
| **Kontrola aplikacji** | | |  |  |
| 58. | | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | TAK |  |
| 59. | | Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | TAK |  |
| 60. | | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, takich jak pobieranie, wysyłanie plików. | TAK |  |
| 61. | | Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. | TAK |  |
| 62. | | Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | TAK |  |
| **Kontrola WWW** | | |  |  |
| 63. | | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. | TAK |  |
| 64. | | W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. | TAK |  |
| 65. | | Filtr WWW musi dostarczać kategorii stron zabronionych prawem: np. Hazard. | TAK |  |
| 66. | | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. | TAK |  |
| 67. | | Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. | TAK |  |
| 68. | | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. | TAK |  |
| 69. | | W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | TAK |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | | |  |  |
| 70. | | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. | TAK |  |
| 71. | | Powinna istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. | TAK |  |
| 72. | | Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. | TAK |  |
| 73. | | Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | TAK |  |
| **Zarządzanie** | | |  |  |
| 74. | | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. | TAK |  |
| 75. | | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. | TAK |  |
| 76. | | Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. | TAK |  |
| 77. | | System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. | TAK |  |
| 78. | | System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. | TAK |  |
| 79. | | Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. | TAK |  |
| 80. | | Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | TAK |  |
| **Logowanie** | | |  |  |
| 81. | | Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. | TAK |  |
| 82. | | W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. | TAK |  |
| 83. | | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. | TAK |  |
| 84. | | Musi istnieć możliwość logowania do serwera SYSLOG. | TAK |  |
| **Serwisy i licencje** | | |  |  |
| 85. | Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów (dostarczone wraz ze sprzętem). Powinny one obejmować:   * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 36 miesięcy. | | TAK |  |
| **Opisy do wymagań ogólnych** | | |  |  |
| 86. | Wykonawca winien przedłożyć wraz ze sprzętem dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. | | TAK |  |
| **Gwarancja oraz wsparcie** | | |  |  |
| 87. | | **Gwarancja min. 36 miesięcy.** | TAK, podać |  |
| 88. | | Zamawiający oczekuje dostarczenia zamówionych urządzeń do 14 dni od momentu złożenia zamówienia. | TAK |  |
| 89. | | Wykonawca powinien posiadać minimum 2 certyfikowanych inżynierów w zakresie instalacji i konfiguracji systemu bezpieczeństwa oferowanego producenta. Certyfikaty inżynierów wykonawca będzie zobowiązany przedstawić na każde żądanie zamawiającego. | TAK |  |
| 90. | | Serwis polegający na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24h x 7dni. | TAK |  |
| 91. | | W okresie gwarancyjnym czas reakcji serwisu, tj. od chwili powiadomienia do rozpoczęcia naprawy wyniesie maksymalnie 1 dzień roboczy. | TAK |  |
| 92. | | Czas skutecznej naprawy max. 5 dni roboczych licząc od dnia zgłoszenia | TAK |  |
| 93. | | Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do zapewnienia dla co najmniej dwóch pracowników zamawiającego, szkolenia (prowadzonego przez autoryzowanego trenera producenta), z zakresu obsługi i konfiguracji systemu bezpieczeństwa dostarczonego w ramach zamówienia. | TAK |  |
| 94. | | Deklaracja zgodności lub certyfikat CE | TAK |  |
| 95. | | Dostępność części zamiennych oraz wyposażenia eksploatacyjnego min. 3 lat od daty uruchomienia | TAK, podać |  |

UWAGA!

Wykonawca zobowiązany jest wypełnić wszystkie wiersze w kolumnie „Parametr oferowany”, przy czym:

a) W przypadku, gdy Zamawiający wymaga podania parametru w formie wartości liczbowej, Wykonawca winien podać wartość cyfrowo;

b) W przypadku, gdy Zamawiający wymaga podania parametru w formie wartości słownej, Wykonawca winien podać wartość słownie, wpisując odpowiednie sformułowanie lub opis;

c) W przypadku, gdy Zamawiający wymaga określenia czy sprzęt posiada lub nie posiada danego parametru, Wykonawca winien wpisać odpowiednio TAK lub NIE;

Oferta Wykonawcy, który nie wpisze żadnej wartości odpowiednio liczbowej/słownej/sformułowania TAK lub NIE, w obrębie poszczególnych parametrów, wpisze wartość parametru powyżej maksimum lub poniżej minimum (w zależności od parametru) określonego przez Zamawiającego lub wpisze, że sprzęt nie posiada parametru, w przypadku, gdy będzie on obligatoryjny, zostanie odrzucona na podstawie art. 226 ust. 1 pkt 5 PZP.

..................................................................

miejscowość i data

Formularz podpisany przy pomocy podpisu elektronicznego

dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub osobistym

Zamawiający zaleca zapisanie dokumentu w formacie PDF