**ZAPROSZENIE DO SKŁADANIA OFERT**

**na realizację Przedsięwzięcia pn.”Wdrożenie e-Usług w placówce POZ” na mocy Umowy nr UM.POZ2.U-9904.2022-00/2199/2023/125 o powierzenie Grantu**

CPV 32424000-1 Infrastruktura sieciowa

1. **Zamawiający**

Powiatowe Centrum Zdrowia sp. z o.o. zs. w Brzezinach (95-060) przy ul. M. Skłodowskiej – Curie 6, KRS: 0000314018, NIP: 833-138-44-12, REGON: 100576369

1. **Adres inwestycji**

Przychodnia Rejonowa – POZ, ul. Bohaterów Warszawy 2, 95-060 Brzeziny, Gmina Brzeziny, Powiat Brzeziński, województwo łódzkie

1. **Cel inwestycji**

Celem inwestycji jest zapewnienie infrastruktury niezbędnej do wdrożenia e-Usług w POZ.

Celem postępowania jest wyłonienie dostawcy zapory UTM.

1. **Zakres rzeczowy postępowania - parametry:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany parametr**  **TAK/OPCJONALNIE** |
| 1. | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza | TAK |
| 2. | System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN | TAK |
| 3. | W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewalla, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji | TAK |
| 4. | Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu | TAK |
| 5. | System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall * ochrony w warstwie aplikacji * protokołów routingu dynamicznego | TAK |
| 5. | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. | 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 |
| 10. | System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45 | TAK |
| 11. | System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB | TAK |
| 12. | 1. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q | TAK |
| 13. | System musi być wyposażony w zasilanie AC | TAK |
| 14. | W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę | TAK |
| 15. | Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B | TAK |
| 16. | Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps | TAK |
| 17. | Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps | TAK |
| 18. | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps | TAK |
| 19. | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps | TAK |
| 20. | Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 Mbps | TAK |
| 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. | Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) | 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. | 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 |
| 33. | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. | TAK |
| 34. | System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu i dedykowany ALG (Application Level Gateway) dla protokołu SIP. | TAK |
| 35. | W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. | TAK |
| 36. | Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. | TAK |
| 37. | Dedykowany ALG (Application Level Gateway) dla protokołu SIP. | TAK |
| 38. | Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), OpenStack, VMware NSX. | TAK |
| 39. | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: wsparcie dla IKE v1 oraz v2, obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), obsługa protokołu Diffie-Hellman grup 19 i 20, wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla  dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, 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 (np. OSPF) oraz routingu statycznego, obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth, mechanizm „Split tunneling” dla połączeń Client-to-Site. | TAK |
| 40. | 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. | TAK |
| 41. | 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 |
| 42. | System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN | TAK |
| 43. | Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu | TAK |
| 44. | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu | TAK |
| 45. | Musi istnieć możliwość określania pasma dla poszczególnych aplikacji | TAK |
| 46. | System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL | TAK |
| 47. | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) | TAK |
| 48. | System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR | TAK |
| 49. | System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android) | TAK |
| 50. | 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 |
| 51. | System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików | TAK |
| 52. | Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta | TAK |
| 53. | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych | TAK |
| 54. | System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach | TAK |
| 55. | Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora | TAK |
| 56. | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur | TAK |
| 57. | System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS | TAK |
| 58. | 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 |
| 59. | Wykrywanie i blokowanie komunikacji C&C do sieci botnet | TAK |
| 60. | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP | TAK |
| 61. | Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora | TAK |
| 62. | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików | TAK |
| 63. | Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P | TAK |
| 64. | Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur | TAK |
| 65. | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne | TAK |
| 66. | 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 |
| 67. | Filtr WWW musi dostarczać kategorii stron zabronionych prawem | TAK |
| 68. | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL | TAK |
| 69. | Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo | TAK |
| 70. | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania | TAK |
| 71. | W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji | TAK |
| 72. | 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 |
| 73. | Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego | TAK |
| 74. | Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API | TAK |
| 75. | Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP | TAK |
| 76. | 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 |
| 77. | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów | TAK |
| 78. | Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego | TAK |
| 79. | 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 |
| 80. | System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację | TAK |
| 81. | Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall | TAK |
| 82. | 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 |
| 83. | Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze producenta, z funkcją rocznej retencji logów | TAK |
| 84. | 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 |
| 85. | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu | TAK |
| 86. | Musi istnieć możliwość logowania do serwera SYSLOG | TAK |
| 87. | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall | TAK |
| 88. | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. 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 oraz chmurowy system logowania na okres 12 miesięcy | TAK |
| 89. | System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym 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 24x7 | TAK |
| 90. | Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty | TAK |

Jeżeli w powyższym opisie przedmiotu zamówienia znajdują się wskazania znaków towarowych, patentów lub pochodzenia, należy przyjąć, że wskazaniu takiemu towarzyszą wyrazy „lub równoważny”.Dopuszcza się więc wszelkie równoważne odpowiedniki rynkowe o właściwościach nie gorszych niż wskazane. Parametry wskazanego standardu określają minimalne warunki techniczne, eksploatacyjne, użytkowe, jakościowe   
i funkcjonalne, jakie ma spełnić przedmiot zamówienia. Wskazane znaki towarowe, patenty, marki lub nazwy producenta wskazujące na pochodzenie określają jedynie klasę produktu, metody, materiałów, urządzeń, systemów, technologii itp. Można więc przyjąć metody, materiały, urządzenia, systemy, technologie itp. innych marek i producentów, jednak o parametrach technicznych, jakościowych i właściwościach użytkowych   
oraz funkcjonalnych odpowiadających metodom, materiałom, urządzeniom, systemom   
i technologiom itp. powyżej opisanym. Dodatkowo Zamawiający podkreśla,   
że równoważne metody, materiały, urządzenia, systemy, technologie itp. nie mogą stanowić zamienników w stosunku do metod, materiałów, urządzeń, systemów, technologii itp. opisanych w dokumentacji za pomocą znaków towarowych, patentów, pochodzenia.

1. **Termin realizacji inwestycji**

Do dnia 31.05.2023 r.

1. **Warunki realizacji inwestycji**
2. Termin i miejsce dostawy muszą być uzgodnione z Kierownikiem Działu IT   
   (tel. 511 856 818, e-mail: s.rzeznicki@szpital-brzeziny.pl.
3. Dostarczona wraz ze sprzętem dokumentacja techniczno – rozruchowa   
   oraz potwierdzająca udzielenie gwarancji musi być sporządzona w języku polskim.
4. Odbiór dostarczonych pozycji zostanie potwierdzony protokołem.
5. **Kryteria oceny ofert**
6. Cena – 100%

W kryterium „Cena” oferta otrzyma zaokrągloną do dwóch miejsc po przecinku liczbę punktów wynikająca z następującego działania:

Wkc=(Cmin/Cof) x 100 x Wk, gdzie:

Wkc – wartość kryterium „Cena”

Cmin – najniższa cena brutto zaoferowana w postępowaniu

Cof – cena brutto zaproponowana przez Oferenta

Wk – waga kryterium (100%)

1. **Sposób przygotowania oferty**

Ofertę należy przygotować poprzez szczegółowe wypełnienie i podpisanie formularza oferty. Oferent może załączyć do oferty katalog/i opisujący/e proponowane sprzęt.

**Uwaga:**

Zamówienie nie może być udzielone podmiotom powiązanym z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:

1. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
2. posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika  
   z przepisów prawa lub nie został określony przez IZ PO,
3. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia   
   w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

W celu spełnienia powyższego warunku, Oferent jest zobowiązany wraz z ofertą złożyć oświadczenie, którego wzór stanowi Załącznik nr 3 do niniejszego zaproszenia ofertowego.

1. **Termin i sposób składania ofert**

Oferty należy złożyć w terminie do 31.03.2023 r. na adres [a.kurzynska@szpital-brzeziny.pl](mailto:a.kurzynska@szpital-brzeziny.pl).

Ofertę stanowi wypełniony i podpisany formularz oferty. Złożenie oferty jest jednoznaczne z akceptacją projektu umowy, stanowiącego załącznik do zaproszenia do składania ofert.

1. **Osoby do kontaktu**

Aneta Kurzyńska – Kierownik ds. inwestycji i administracji budynkami, tel. 500 044 688, e-mail: [a.kurzynska@szpital-brzeziny.pl](mailto:a.kurzynska@szpital-brzeziny.pl); Sławomir Rzeźnicki – Kierownik Działu IT, tel. 511 856 818, e-mail: s.rzeznicki@szpital-brzeziny.pl

1. **Załączniki**
2. Formularz oferty
3. Projekt umowy
4. Oświadczenie Oferenta o braku powiązań kapitałowych i osobowych z Zamawiającym