*Załącznik nr 1*

*Nr sprawy: KF-Z.45.2023*

**FORMULARZ OFERTOWY**

Nazwa Wykonawcy: .......................................................................................................................................................................

Adres Wykonawcy: ........................................................................................................................................................................

NIP…………………………………………………………………… REGON ................................................................................

Nr telefonu: ...................................................Nr faxu ............................................ adres e΄mail …………..……………………….

Odpowiadając na zaproszenie do składania ofert w postępowaniu o udzielenie zamówienia o wartości szacunkowej netto nie przekraczającej 130 000 zł, na: dostawę systemów bezpieczeństwa poczty elektronicznej, stacji roboczych i serwerów, systemu EDR, a także rozwój obecnej zapory sieciowej (Firewall) dla Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Krasnymstawie proponujemy realizację zamówienia na następujących warunkach:

Cena netto………………………………………………………………………………………………..

Stawka VAT………………………………………………………………………………………………..

Cena brutto…………………………………………………………………………………………………

Słownie brutto:……………………………………………………………………………………………………………………………………………………………………………………………………

Producent: …………………………………………………………………………………………………………………………………………………………………………

Typ/model urządzenia……………………………………………………………………………………………………………………………………………………………

Kraj pochodzenia…………………………………………………………………………………………………………………………………………………………………

**Dostawa oprogramowania poczty elektronicznej wraz z systemem bezpieczeństwa:**

## **Wymagania systemu:**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| 1. | System musi umożliwiać skanowanie minimum 250 adresów mailowych bez limitu liczby domen. | **TAK** |  |
| 2. | System musi posiadać konsolę zarządzającą dostępną przez przeglądarkę internetową. | **TAK** |  |
| 3. | System musi umożliwiać dostęp do konsoli osobno poprzez http oraz https | **TAK** |  |
| 4. | System musi mieć możliwość implementacji wewnątrz i na zewnątrz struktury informatycznej organizacji, powinien funkcjonować niezależnie od pozostałych jej elementów. | **TAK** |  |
| 5. | Rozwiązanie musi wspierać filtrację dla serwerów znajdujących się wewnątrz i na zewnątrz struktury informatycznej danej organizacji. | **TAK** |  |
| 6. | System musi być dostępny w postaci pliku ISO pozwalającym na instalację na serwerze fizycznym, jak też w wersji na maszyny wirtualne ze wsparciem dla następujących środowisk: VMWare, Citrix, MS Hyper-V. | **TAK** |  |
| 7. | Interfejs rozwiązania musi wspierać kilka języków i posiadać także polskojęzyczny interfejs. | **TAK** |  |
| 8. | System musi zawierać główny pulpit, na którym będą wyświetlane podstawowe informacje takie jak:   * 1. Stan systemu w tym zużycie CPU, RAM, pamięci dyskowej ,   2. Wersję systemu i bieżącą datę,   3. Informacje o typie aktualnie używanego procesora ,   4. Informacje o stanie skanerów antywirusowych,   5. Wykres przedstawiający informacje zbiorcze na temat procesowania wiadomości,   6. Informacje z ostatnich siedmiu dni w formie listy lub/i wykresu przedstawiające liczbę zablokowanych wiadomości, liczbę wystąpień wirusów, liczbę zablokowanych załączników i innych odrzuceń,   7. Listy najpopularniejszych nadawców wirusów i spamu oraz najpopularniejszych wirusów wykrytych przez silniki antywirusowe. | **TAK** |  |
| 9. | System musi w widocznym miejscu zawierać sekcje poświęconą wsparciu technicznemu umożliwiającą utworzenie bezpiecznego połączenia z suportem producenta. | **TAK** |  |
| 10. | Konsola zarządzająca musi mieć możliwość dostosowywania wyglądu, personalizacji kolorystyki interfejsu i umieszczenia logo firmy. | **TAK** |  |
| 11. | System musi mieć możliwość obsługi certyfikatów SSL. | **TAK** |  |
| 12. | System musi mieć możliwość importu certyfikatów. | **TAK** |  |
| 13. | * System musi mieć możliwość obsługi TLS. | **TAK** |  |
| 14. | System musi mieć funkcjonalność szyfrowania emaili kluczem prywatnym, i odszyfrowywania ich u odbiorcy kluczem publicznym, tak zwane **DKIM** | **TAK** |  |
| 15. | System musi mieć możliwość uwierzytelniania nadawcy poprzez określone mechanizmy, nie mniej niż **SPF, DMARC, ARC.** | **TAK** |  |
| 16. | System musi mieć możliwość wykonywania kopii zapasowych konfiguracji zarówno automatycznych na serwerze FTP lub w chmurze amazona, jak i na żądanie, a także możliwość importu takiej konfiguracji. | **TAK** |  |
| 17. | System musi obsługiwać zdalny Syslog, osobny dla logów dotyczących maili i osobny dla logów dotyczących inferface’u oraz zmian w systemie | **TAK** |  |
| 18. | System musi wspierać SNMP v2c oraz v3 | **TAK** |  |
| 19. | System musi mieć możliwość pracy w klastrze (dwóch lub więcej węzłów). | **TAK** |  |
| 20. | Aktualizacja systemu musi odbywać się poprzez konsolę webową, oraz nie może mieć wpływu na działanie samego systemu (tj. żadna wiadomość mailowa nie zostanie utracona). W przypadku aktualizacji systemów działających w klastrze, musi istnieć możliwość uruchomienia tych procesów oddzielnie (np. w przypadku gdyby aktualizacja okazała się wadliwa) | **TAK** |  |
| 21. | System musi posiadać wbudowany silnik antyspamowy. | **TAK** |  |
| 22. | System musi mieć umożliwiać korzystanie z zewnętrznych baz RBL, dowolnie definiowanych przez administratora. | **TAK** |  |
| 23. | System musi mieć możliwość tworzenia przez administratora białej listy adresów IP nadawcy, pomijanych podczas filtracji RBL. | **TAK** |  |
| 24. | System musi mieć możliwość wyłączania filtracji RBL dla poszczególnych domen podpiętych do rozwiązania. | **TAK** |  |
| 25. | System musi mieć możliwość sprawdzenia poprawności odbiorcy danej wiadomości, w trybie co najmniej: dynamicznym (weryfikacja na serwerze docelowym), LDAP, listę dozwolonych odbiorców oraz poprzez wyrażenia regularne. | **TAK** |  |
| 26 | System musi być wspierany samouczącą się bazą danych Bayes’a. | **TAK** |  |
| 27. | System musi obsługiwać Passive OS Fingerprinting oraz mechanizm Penpals i analizę Botnetów. | **TAK** |  |
| 28. | System musi posiadać konfigurowalną szarą listę, z możliwością jej włączenia i wyłączenia | **TAK** |  |
| 29. | System musi pozwalać na zdefiniowanie języków, w których to muszą być napisane wiadomości, by pomyślnie przeszły weryfikację | **TAK** |  |
| 30. | System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach email oraz nazwach domen. Listy powinny być traktowane globalnie, per domena i osobno dla każdego użytkownika. | **TAK** |  |
| 31. | System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach IP serwerów pocztowych nadawcy. | **TAK** |  |
| 32. | System musi mieć możliwość indywidualnego ustalania wysokości progu filtrowania wiadomości przez moduł antyspamowy dla domen jak i również dla określonych aliasów pocztowych. | **TAK** |  |
| 33. | System musi mieć możliwość rozczytywania skróconych wersji URLi | **TAK** |  |
| 34. | System musi mieć możliwość dodawania konfigurowalnych stopek do maili wychodzących, które potwierdzą że zostały one przefiltrowane przez tenże system | **TAK** |  |
| 35. | System musi zawierać dwa niezależnie działające silniki antywirusowe zewnętrznego dostawcy. | **TAK** |  |
| 36. | System musi mieć możliwość całkowitego wyłączenia silnika antywirusowego. | **TAK** |  |
| 37. | System musi samoczynnie aktualizować bazę danych dla wbudowanego silnika antywirusowego. Baza musi być aktualizowana minimum, co godzinę. | **TAK** |  |
| 38. | System musi umożliwiać blokowanie wybranych przez administratora rozszerzeń i nazw plików. | **TAK** |  |
| 39. | System musi umożliwiać blokowanie co najmniej następujących rozszerzeń plików:  ade, adp, bat, chm, cmd, com, cpl, dll, doc, exe, hta, ins, isp, jar, js, jse, lib, lnk, mde, msc, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh | **TAK** |  |
| 40. | System musi umożliwiać blokowanie co najmniej następujących typów MIME:  application/ecmascript, application/javascript, application/x-javascript,  application/x-msdos-program, application/x-msdownload, text/ecmascript,  text/javascript | **TAK** |  |
| 41. | Wykrywanie i blokowanie rozszerzenia załącznika typu wykonywalnego powinno być odporne na zmianę nazwy i rozszerzenia, również w przypadku skompresowanego archiwum. | **TAK** |  |
| 42. | System musi umożliwiać blokowanie zabezpieczonych hasłem archiwów. | **TAK** |  |
| 43. | System musi umożliwiać tworzenie własnych reguł filtracji. | **TAK** |  |
| 44. | System musi umożliwiać kontrolę treści opartej na słowniku lub wyrażeniu regularnym (przykładowo blokowanie wiadomości z numerami kard kredytowych, numerami PESEL czy też innymi danymi określanymi jako wrażliwe). | **TAK** |  |
| 45. | Wszystkie wyżej wymienione funkcje powinny być dostępne dla filtracji wiadomości wychodzących i przychodzących. | **TAK** |  |
| 46. | System musi posiadać mechanizm przepisywania linków w wiadomościach, automatycznie kierujący odbiorcę na serwery zewnętrzne, które kategoryzują strony internetowe pod kątem zagrożeń:  a. Funkcjonalność można ustawić osobno dla domeny i dla użytkownika systemu  b. Można tworzyć wyjątki dla domen stron internetowych, które mają być nie przepisywane, osobno dla całej domeny pocztowej oraz użytkowników systemu.  c. Funkcjonalność powinna pozwalać na edycję wyświetlanej strony z informacją o blokadzie, minimum o treść wyświetlanej informacji oraz o wyświetlane logo. | **TAK** |  |
| 47. | System musi posiadać moduł powiadamiający adresata bądź odbiorcę wiadomości o podjętych przez system akcjach. | **TAK** |  |
| 48. | System musi powiadamiać o zablokowanych wiadomościach w tym wiadomościach zablokowanych przez moduł antyspamowy, antywirusowy czy moduł kontroli treści. | **TAK** |  |
| 49. | Wiadomości powinny być edytowalne i wysyłane do odbiorcy lub/i nadawcy. | **TAK** |  |
| 50. | System musi posiadać mechanizm kwarantanny. | **TAK** |  |
| 51. | System musi zawierać wbudowaną wyszukiwarkę. | **TAK** |  |
| 52. | System musi generować raporty kwarantanny  a. Raporty kwarantanny powinny być generowane automatycznie lub na żądanie  b. Raporty kwarantanny powinny być personalizowane (w tym podmiana logo producenta)  c. Raporty powinny być generowane dla użytkowników systemu pocztowego.  d. W przypadku współpracy z serwerami pocztowymi Microsoft Exchange, raport powinien być generowany dla użytkownika tylko raz, uwzględniając jego wszystkie aliasy. | **TAK** |  |
| 53. | System musi umożliwić dostęp do kwarantanny poprzez interfejs przeglądarki internetowej dla każdego użytkownika indywidualnie z możliwością dopasowania odpowiednich uprawnień. | **TAK** |  |
| 54. | System musi umożliwić uwierzytelnianie użytkownika za pośrednictwem wewnętrznej bazy, LDAP, w oparciu o bazę kont na docelowym serwerze pocztowym (POP3, IMAP), lub bazy SQL. | **TAK** |  |
| 55. | System musi mieć możliwość tworzenie wielu administratorów o zróżnicowanym poziomie uprawnień. | **TAK** |  |
| 56. | System musi mieć możliwość tworzenia grup domen przyporządkowanych odpowiednim administratorom. | **TAK** |  |
| 57. | System musi posiadać funkcję kontroli ilości przetwarzanych wiadomości dla ruchu przychodzącego i wychodzącego. | **TAK** |  |
| 58. | System musi umożliwiać wyświetlanie statystyk dotyczących aktualnego użycia licencji (liczby unikalnych kont mailowych, przez które przechodzą wiadomości). | **TAK** |  |
| 59. | System musi umożliwiać manualne ustawienie równocześnie pracujących procesów SMTP w celu optymalizacji wydajności rozwiązania względem platformy, na której jest zainstalowane. | **TAK** |  |
| 60. | System musi posiadać moduł kontroli jakości, który pozwoli zdefiniować ograniczenia odnoszące się do co najmniej:  a. ilości maili, które mogą zostać wysłane z określonej jednostce czasu  b. zbiorczego rozmiaru maili, które mogą zostać wysłane w określonej jednostce czasu. | **TAK** |  |
| 61. | System musi mieć możliwość ujednolicenia aliasów emailowych | **TAK** |  |
| 62. | System powinien mieć możliwość konfiguracji raportów generowanych użytkownikom tak, aby mogły być generowane na żądanie (z opcją wyłączenia tej opcji przez administratora). | **TAK** |  |

## **Szkolenia systemu bezpieczeństwa poczty elektronicznej:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Wykonawca zapewni w ramach realizacji zamówienia przeszkolenie dla 3 osób – administratorów z zakresu obsługi dostarczanego rozwiązania. | **TAK** |  |

## **Usługi systemu bezpieczeństwa poczty elektronicznej:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Usługi instalacyjne, konfiguracja oraz wdrożenie. | **TAK** |  |

## **Gwarancja i licencje systemu bezpieczeństwa poczty elektronicznej:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Gwarancja systemu poczty elektronicznej wraz z systemem bezpieczeństwa:  24 miesiące. W tym bezpłatna pomoc techniczna. | **TAK** |  |
| Niezbędne licencje dla minimum 250 adresów mailowych  Okres ważności licencji - 24 miesiące, licząc od dnia odbioru przez Zamawiającego. | **TAK** |  |

**Dostawa oprogramowania ochrony stacji roboczych i serwerów, systemu Endpoint Detection and Response w architekturze serwera:**

# **Wymagania ogólne sytemu:**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| **System Endpoint Detection and Response w architekturze serwera:** | | | |
| 1. | Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta | **TAK** |  |
| 2. | Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta | **TAK** |  |
| 3. | Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta | **TAK** |  |
| 4. | Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa | **TAK** |  |
| 5. | Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica” | **TAK** |  |
| 6. | Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia | **TAK** |  |
| 7. | Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika | **TAK** |  |
| 8. | Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku | **TAK** |  |
| 9. | Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania | **TAK** |  |
| 10. | Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł | **TAK** |  |
| 11. | Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli | **TAK** |  |
| 12. | Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell | **TAK** |  |
| **Administracja zdalna:** | | | |
| 13. | Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD | **TAK** |  |
| 14. | Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL | **TAK** |  |
| 15. | Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta | **TAK** |  |
| 16. | Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL | **TAK** |  |
| 17. | Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów | **TAK** |  |
| 18. | Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi | **TAK** |  |
| 19. | Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci | **TAK** |  |
| 20. | Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) | **TAK** |  |
| 21. | Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT | **TAK** |  |
| 22. | Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej | **TAK** |  |
| 23. | Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów | **TAK** |  |
| 24. | Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera | **TAK** |  |
| 25. | * Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora | **TAK** |  |
| 26. | Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog | **TAK** |  |
| 27. | Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami | **TAK** |  |
| **Ochrona stacji roboczych:** | | | |
| 28. | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows7/Windows 10/Windows 11) | **TAK** |  |
| 29. | Rozwiązanie musi wspierać architekturę ARM64 | **TAK** |  |
| 30. | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor | **TAK** |  |
| 31. | Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet | **TAK** |  |
| 32. | Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji | **TAK** |  |
| 33. | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików | **TAK** |  |
| 34. | Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu | **TAK** |  |
| 35. | Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych | **TAK** |  |
| 36. | Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku | **TAK** |  |
| 37. | Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego) | **TAK** |  |
| 38. | Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS | **TAK** |  |
| 39. | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie | **TAK** |  |
| 40. | Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych | **TAK** |  |
| 41. | Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia | **TAK** |  |
| 42. | Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:  tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,  • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,  • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,  • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,  • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. | **TAK** |  |
| 43. | Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników | **TAK** |  |
| 44. | Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa | **TAK** |  |
| 45. | Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji | **TAK** |  |
| 46. | Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne) | **TAK** |  |
| 47. | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego | **TAK** |  |
| 48. | Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook | **TAK** |  |
| 49. | Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,  • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,  • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,  • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. | **TAK** |  |
| 50. | Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki | **TAK** |  |
| 51. | Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika | **TAK** |  |
| 52. | Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki | **TAK** |  |
| 53. | Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych | **TAK** |  |
| 54. | Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii | **TAK** |  |
| 55. | Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day | **TAK** |  |
| 56. | W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum | **TAK** |  |
| **Ochrona serwera:** | | | |
| 57. | Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux | **TAK** |  |
| 58. | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami | **TAK** |  |
| 59. | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor | **TAK** |  |
| 60. | Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS | **TAK** |  |
| 61. | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie | **TAK** |  |
| 62. | Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji | **TAK** |  |
| 63. | Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów | **TAK** |  |
| 64. | Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty | **TAK** |  |
| **Dodatkowe wymagania:** | | | |
| 65. | Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive | **TAK** |  |
| 66. | Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS) | **TAK** |  |
| 67. | Rozwiązanie musi wspierać skanowanie magazynu Hyper-V | **TAK** |  |
| 68. | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego | **TAK** |  |
| 69. | Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych | **TAK** |  |
| 70. | Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki | **TAK** |  |
| 71. | Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych | **TAK** |  |
| 72. | Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP | **TAK** |  |
| 73. | Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu | **TAK** |  |
| 74. | Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej | **TAK** |  |
| 75. | Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web | **TAK** |  |
| 76. | Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon | **TAK** |  |
| 77. | Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu | **TAK** |  |
| **Szyfrowanie:** | | | |
| 78. | System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit | **TAK** |  |
| 79. | System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) | **TAK** |  |
| 80. | Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia | **TAK** |  |
| 81. | Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI | **TAK** |  |
| **Ochrona urządzeń mobilnych opartych o system Android:** | | | |
| 82. | Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie | **TAK** |  |
| 83. | Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne | **TAK** |  |
| 84. | Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki) | **TAK** |  |
| 85. | Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji | **TAK** |  |
| 86. | Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:  a. nazwę aplikacji,  b. nazwę pakietu,  c. kategorię sklepu Google Play,  d. uprawnienia aplikacji,  e. pochodzenie aplikacji z nieznanego źródła. | **TAK** |  |

## **Szkolenia systemu:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Wykonawca zapewni w ramach realizacji zamówienia przeszkolenie dla 3 osób – administratorów z zakresu obsługi dostarczanego rozwiązania. | **TAK** |  |

## **Usługi systemu:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Usługi instalacyjne, konfiguracja oraz wdrożenie. | **TAK** |  |

## **Gwarancja i licencje systemu:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Gwarancja systemu: 24 miesiące. W tym bezpłatna pomoc techniczna. | **TAK** |  |
| Niezbędne licencje dla 330 stanowisk. Okres ważności licencji - 24 miesiące, licząc od dnia odbioru przez Zamawiającego. | **TAK** |  |

**Rozwój obecnej zapory sieciowej (Firewall) poprzez dostarczenie nowego urządzenia UTM oraz utworzenia klastra HA:**

|  |
| --- |
| **Wymagania ogólne Firewall:** |
| Dostarczone systemy bezpieczeństwa muszą zapewniać wszystkie wymienione poniżej funkcje. 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. |

# **Funkcje modułu Firewall:**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| 1. | Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive. | **TAK** |  |
| 2. | Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2). | **TAK** |  |
| 3. | Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode). | **TAK** |  |
| 4. | Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4. | **TAK** |  |
| 5. | Musi obsługiwać Multicast routing. | **TAK** |  |
| 6. | Musi obsługiwać Policy Based routing. | **TAK** |  |
| 7. | Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług. | **TAK** |  |
| 8. | Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie. | **TAK** |  |
| 9. | Musi obsługiwać DHPCv6 na zewnętrznym interfejsie. | **TAK** |  |
| 10. | Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup). | **TAK** |  |
| 11. | Musi obsługiwać Dynamic DNS. | **TAK** |  |
| 12. | Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1. | **TAK** |  |
| 13. | * Musi obsługiwać translację portów: PAT. | **TAK** |  |
| 14. | Musi obsługiwać IPSec NAT traversal. | **TAK** |  |
| 15. | Musi obsługiwać mechanizm Policy Based NAT. | **TAK** |  |
| 16. | Musi obsługiwać VLAN 802.1Q. | **TAK** |  |
| 17. | Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych. | **TAK** |  |
| 18. | Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP. | **TAK** |  |
| 19. | Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB. | **TAK** |  |
| 20. | Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich. | **TAK** |  |
| 21. | Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi. | **TAK** |  |
| 22. | Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza. | **TAK** |  |
| 23. | Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów. | **TAK** |  |
| 24. | Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego. | **TAK** |  |
| 25 | Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników. | **TAK** |  |
| 26. | Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory. | **TAK** |  |
| 27. | Urządzenie musi posiadać co najmniej 2 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory. | **TAK** |  |
| 28. | Co najmniej jedna metoda transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta na stacjach roboczych użytkowników. | **TAK** |  |
| 29. | Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix. | **TAK** |  |
| 30. | Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej. | **TAK** |  |
| 31. | Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji. | **TAK** |  |
| 32. | Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen. | **TAK** |  |
| 33. | Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów. | **TAK** |  |
| 34. | Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej. | **TAK** |  |
| 35. | Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http. | **TAK** |  |
| 36. | Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP. | **TAK** |  |
| 37. | Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP. | **TAK** |  |
| 38. | Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów. | **TAK** |  |
| 39. | Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site. | **TAK** |  |

## **Parametry fizyczne systemu Firewall:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Element systemu pełniący funkcję Firewall musi dysponować :   * 8 portami 1Gb RJ45. * System powinien umożliwiać rozbudowę o dodatkowe porty: 4 x SFP lub   2 x SFP+ lub 8 x RJ45.   * Minimum 8 GB pamięci RAM. * Minimum 2 porty USB 3.0. * Minimum jeden port typu Console. | **TAK** |  |

## **Parametry wydajnościowe systemu Firewall:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| * Przepustowość Firewall minimum: 18 Gbps. * Przepustowość IPSec VPN nie mniejsza niż: 5.2 Gbps. * Przepustowość skanowania antywirusowego nie mniejsza niż: 3.1 Gbps. * Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 3.3 Gbps. * Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 2.4 Gbps. * Obsługa nie mniej niż: 250 tuneli IPSec site-to-site. * Obsługa nie mniej niż: 250 tuneli client-to-site. * Obsługa nie mniej niż: 4.500.000 jednoczesnych połączeń. * Obsługa nie mniej niż: 98.000 nowych połączeń na sekundę. * W ramach Firewall system musi obsługiwać minimum: 250 sieci VLAN. | **TAK** |  |

## **Wymagane funkcje VPN systemu Firewall:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| * Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE. * W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów. * Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256. * Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty. * Obsługa Dead Peer Detection (DPD). * Wsparcie dla IKEv1 i IKEv2. * Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman. * Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego). * Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu. * Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2. * Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android. * Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows. * Dla połączeń Client-to-Site możliwość zastosowania dwuskładnikowego uwierzytelnienia w oparciu o tokeny sprzętowe lub programowe. | **TAK** |  |

# **Zarządzanie Firewall:**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| 1. | Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www. | **TAK** |  |
| 2. | Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach. | **TAK** |  |
| 3. | Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji. | **TAK** |  |
| 4. | W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny). | **TAK** |  |
| 5. | Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie. | **TAK** |  |
| 6. | Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania. | **TAK** |  |
| 7. | Komunikacja do systemów logowania i raportowania musi być szyfrowana. | **TAK** |  |
| 8. | W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania. | **TAK** |  |

# **Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania Firewall:**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| 1. | Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów. | **TAK** |  |
| 2. | Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów. | **TAK** |  |
| 3. | Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online | **TAK** |  |
| 4. | Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu. | **TAK** |  |
| 5. | Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia. | **TAK** |  |
| 6. | Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie. | **TAK** |  |
| 7. | Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie. | **TAK** |  |
| 8. | System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi. | **TAK** |  |
| 9. | Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail. | **TAK** |  |
| 10. | System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów. | **TAK** |  |
| 11. | Rozwiązanie musi zapewniać narzędzie graficznej analizy logów. | **TAK** |  |
| 12. | Umożliwia przeglądanie logów ruchu w czasie rzeczywistym. | **TAK** |  |
| 13. | Rozwiązanie musi udostępniać narzędzie analizy całości ruchu. | **TAK** |  |
| 14. | Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów. | **TAK** |  |
| 15. | Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie. | **TAK** |  |
| 16. | System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV. | **TAK** |  |
| 17. | System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail. | **TAK** |  |
| 18. | Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości. | **TAK** |  |
| 19. | System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów. | **TAK** |  |
| 20. | System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych. | **TAK** |  |
| 21. | Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom. | **TAK** |  |
| 22. | Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów. | **TAK** |  |

## **Szkolenia Firewall:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Wykonawca zapewni w ramach realizacji zamówienia przeszkolenie dla 3 osób – administratorów z zakresu obsługi dostarczanego rozwiązania. | **TAK** |  |

## **Usługi Firewall:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| Wykonawca jest zobowiązany dokonać konfiguracji klastra (HA) o wysokiej dostępności – podpięcie nowego urządzenia z obecnym posiadanym w siedzibie Zamawiającego. Wymogiem budowy klastra HA jest posiadanie urządzeń tego samego modelu i taką samą wersją firmware. Wykonawca zapewni wszystkie usługi instalacyjne, konfiguracyjne oraz wdrożeniowe. | **TAK** |  |

## **Gwarancja i licencje Firewall:**

|  |  |  |
| --- | --- | --- |
| **Parametr / Opis** | **Parametr wymagany** | **Potwierdzenie spełnienia wymogów oraz opis parametrów oferowanych** |
| System musi być objęty serwisem gwarancyjnym producenta przez 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 (świadczone telefonicznie lub poprzez portal). | **TAK** |  |
| Wykonawca dostarczy wymagane licencje producenta dla nowego oraz obecnego urządzenia, które znajduje się w siedzibie Zamawiającego na okres min. 12 miesięcy. | **TAK** |  |

*Parametry określone jako „TAK” są warunkami granicznymi, których niespełnienie spowoduje odrzucenie oferty.*

**Zakres dostawy:**

* Dostawa oprogramowania poczty elektronicznej wraz z systemem bezpieczeństwa, który będzie obejmował mechanizmy SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową (w tym: usługi instalacyjne, konfiguracja, a także szkolenia). Licencja – 2 lata dla 250 użytkowników.
* Dostawa oprogramowania ochrony stacji roboczych i serwerów, systemu Endpoint Detection and Response w architekturze serwera (w tym: usługi instalacyjne, konfiguracja, a także szkolenia). Licencja – 2 lata dla 330 stanowisk
* Rozwój obecnej zapory sieciowej (Firewall) poprzez dostarczenie nowego urządzenia UTM oraz utworzenia klastra HA (w tym: usługi instalacyjne, konfiguracja, a także szkolenia). Licencja – 12 miesięcy.

Oświadczamy, że

1. Oferowane powyżej urządzenie jest kompletne i po zainstalowaniu i uruchomieniu będzie gotowe do pracy zgodnie z przeznaczeniem bez żadnych dodatkowych zakupów inwestycyjnych, z wyłączeniem materiałów eksploatacyjnych.
2. Oświadczamy, że oferowane urządzenie, oprócz spełnienia odpowiednich parametrów funkcjonalnych, gwarantuje bezpieczeństwo pacjentów i personelu medycznego oraz zapewnia wymagany poziom usług medycznych.

………………………………………………. ………………………..

*Miejscowość i data*  *Podpis Wykonawcy*

Oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora danych – Samodzielny Publiczny Zespół opieki Zdrowotnej w Krasnymstawie, ul. Sobieskiego 4, 22-300 Krasnystaw , KRS 0000097765 w celu związanym z prowadzonym postępowaniem „:Dostawa systemów bezpieczeństwa poczty elektronicznej, stacji roboczych i serwerów, systemu EDR, a także rozwój obecnej zapory sieciowej (Firewall) dla Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Krasnymstawie.

Oświadczam, że dane osobowe podaję dobrowolnie i zapoznałem(-am) się z treścią klauzuli informacyjnej stanowiącej Załącznik Nr 2 do zapytania ofertowego w postępowaniu na „ Dostawa systemów bezpieczeństwa poczty elektronicznej, stacji roboczych i serwerów, systemu EDR, a także rozwój obecnej zapory sieciowej (Firewall) dla Samodzielnego Publicznego Zespołu Opieki Zdrowotnej w Krasnymstawie.” w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawiani, który to fakt potwierdzam własnoręcznym podpisem.

1. Oświadczam, że wraz z ofertą składam następujące dokumenty:

……………………………………………………………..

……………………………………………………………………

……………………………………………………………………

…………………………………………………………….. ……………………………………………………

*Miejscowość i data Podpis Wykonawcy*