**"Rozbudowa systemu backup oraz infrastruktury sieciowej o UTM dla „Poddębickiego Centrum Zdrowia" Sp. z o.o. w Poddębicach”**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| KOD CPV: 30233000-1, 48000000-8, 32413100-2. | | | | | | | |
| L.p. | Przedmiot zamówienia | j.m. | Ilość | Cena netto za szt. | Wartość netto  (zł) | Stawka VAT (%) | Wartość brutto  (zł) |
| 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. |
| 1. | Rozbudowa posiadanej biblioteki LTO ActiData ActiLib (SN posiadanej biblioteki: DE64107948) o 1 szt napędu LTO8 | szt. | 1 |  |  |  |  |
| 2. | UTM (HA) | komplet urządzeń | 1 |  |  |  |  |
| 3. | Macierz | komplet | 1 |  |  |  |  |
|  |  |  |  | **Razem:** |  |  |  |

Zamawiający bezwzględnie wymaga, by asortyment zaoferowany przez Wykonawcę w swojej ofercie był oznaczony w sposób bezspornie go identyfikujący. Takie oznaczenie oferowanego asortymentu pozwoli Zamawiającemu jednoznacznie ocenić, czy zaoferowany sprzęt spełnia wymagane parametry minimalne oraz uchroni Wykonawcę prze ewentualnymi skutkami zmiany treści oferty gdy zajdzie konieczność jej wyjaśnienia przez Zamawiającego w przypadku jej niejednoznaczności.

PARAMETRY TECHNICZNE PRZEDMIOTU ZAMÓWIENIA:

1.Rozbudowa posiadanej biblioteki LTO ActiData ActiLib (SN posiadanej biblioteki: DE64107948) o 1 szt. napędu LTO8

**Podać nazwę i producenta oferowanego urządzenia**: **……………………………………………………….(PROSZĘ WYPEŁNIĆ!!!!)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry i właściwości urządzenia** | **Potwierdzenie spełnienia parametru, podać:**  **TAK/NIE** |
|  | Wymagana rozbudowa wraz z instalacją o napęd LTO-8 wyposażony w złącze z interfejsem FC 8GB.  Prędkość zapisu pojedynczego napędu LTO-8 bez kompresji – minimum 300 MB/sek.  Dostarczony napęd musi być objęty 36 miesięczną gwarancją producenta posiadanej biblioteki i nie ma wpływu na gwarancję dotyczącą biblioteki.  Wymaga się aby gwarancja była świadczona w miejscu instalacji urządzenia z czasem reakcji w trybie NBD realizowana przez autoryzowany serwis producenta biblioteki posiadający aktualne certyfikaty ISO9001, ISO14001, ISO27001 obejmujące usługi serwisowe oferowanego urządzenia wraz z potwierdzeniem możliwości przedłużenia gwarancji do 72 miesięcy.  Dostarczany napęd musi być nowy, nie używany, wyprodukowany nie wcześniej niż 4 miesiące przed złożeniem oferty oraz pochodzić z autoryzowanego kanału sprzedaży producenta na terenie Polski. |  |

1. UTM (HA)– 1 komplet urządzeń

**Podać nazwę i producenta oferowanego urządzenia: ……………………………………………………….(PROSZĘ WYPEŁNIĆ!!!!)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry i właściwości urządzenia** | | **Potwierdzenie spełnienia parametru, podać:**  **TAK/NIE**  **Dodatkowo w poz. 20 podać numer telefonu oraz adres** |
| 1 | **Wymagania Ogólne**  System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia. **Urządzenia muszą być dostarczone w klastrze wysokiej dostępności (HA), które działają w dwóch trybach tj. aktywny- aktywny, aktywny- pasywny.**  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę 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 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego.   Zaoferowane rozwiązanie musi pochodzić z autoryzowanego kanału dystrybutora producenta– **wymagane załączenie wraz z ofertą oświadczenie producenta lub dystrybutora lub Wykonawcy.** | |  |
| 2 | **Redundancja, monitoring i wykrywanie awarii**   1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5. System ma pracować w postaci redundantnego klastra. | |  |
| 3 | **Interfejsy, Dysk, Zasilanie:**   1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 16 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 2 gniazdami SFP+ 10 Gbps.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie AC. | |  |
| 4 | **Parametry wydajnościowe:**   1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. 5. 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 2.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. | |  |
| 5 | **Funkcje Systemu Bezpieczeństwa:**  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS  z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | |  |
| 6 | **Polityki, Firewall**   1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje 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.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje 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. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. | |  |
| 7 | | **Połączenia VPN**   1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem  128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman  grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * 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. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  * Pracę w trybie Portal  - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |  |
| 8 | | **Routing i obsługa łączy WAN**  W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |  |
| 9 | | **Funkcje SD-WAN**   1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |  |
| 10 | | **Zarządzanie pasmem**   1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| 11 | | **Ochrona przed malware**   1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  |
| 12 | | **Ochrona przed atakami**   1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL  oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |  |
| 13 | | **Kontrola aplikacji**   1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |  |
| 14 | | **Kontrola WWW**   1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL  pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |
| 15 | | **Uwierzytelnianie użytkowników w ramach sesji**   1. System Firewall umożliwia 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.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
| 16 | | **Zarządzanie**   1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest  realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). |  |
| 17 | | **Zarządzanie**  Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP – **parametr opcjonalny dodatkowo punktowany w kryterium Parametry techniczne: TAK – 5 punktów, NIE – 0 punktów.** |  |
| 18 | | **Logowanie**   1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |  |
| 19 | | **Serwisy i licencje**  Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |  |
| 20 | | **Gwarancja oraz wsparcie**   1. System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie NBD. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.   Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta  w języku polskim w zakresie:   * obsługa procesu RMA u producenta, * zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, * jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta, * dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.   Dostęp do usługi powinien być świadczony przez **dedykowaną infolinię (należy podać numer telefonu)** oraz przez **dedykowany moduł internetowy (należy podać adres).**  Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. |  |
| 21 | | **Usługi**  Instalacja i Uruchomienie zestawu UTM w tym szczególnie instalacja i pełna konfiguracja firewalli według ustaleń wytycznych Zamawiającego. |  |

**3. Macierz – 1 komplet.**

**Podać producenta i nazwę oferowanego urządzenia: ……………………………………………………….(PROSZĘ WYPEŁNIĆ!!!!)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry i właściwości urządzenia** | **Potwierdzenie spełnienia parametru, podać:**  **TAK/NIE**  **Dodatkowo w poz. 67 podać adres internetowy** |
| 1 | Do obowiązków Wykonawcy należy dostawa **Macierzy** do siedziby Zamawiającego, spełniającej minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jej instalacja i konfiguracja do działania z oprogramowaniem Zamawiającego.  Przez macierz dyskową Zamawiający rozumie się zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe macierzy bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami. |  |
| 2 | Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski. Macierz będzie dostarczona ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maksymalnie 4U w tej szafie. |  |
| 3 | Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). |  |
| 4 | Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug NL-SAS i SSD. Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5”). |  |
| 5 | W przypadku konfiguracji macierzy z dwoma kontrolerami wszystkie zewnętrzne połączenia kablowe pomiędzy modułami muszą zapewniać komunikację nawet w przypadku awarii jednej z półek ze wszystkimi pozostałymi półkami/dyskami. Połączenia kablowe pomiędzy modułami zapewniają przepustowość minimum 48Gb/s w ramach pojedynczego połączenia. |  |
| 6 | Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie surowym (tzw. RAW) minimum 2400 TB bez konieczności wymiany zainstalowanych kontrolerów i z zaoferowaną ilością kontrolerów. |  |
| 7 | Macierz musi być wyposażona w minimum:   * Min.5 dysków 2,5” SSD SAS o pojemności 3,84 TB każdy i parametrze DWPD min. 1. Wymaga się skonfigurowania dysków w RAID6 min.3:2. * Min.12 dysków 3,5” NL-SAS 12G o pojemności minimum 18 TB każdy i prędkości obrotowej min 7,2 krpm Wymaga się skonfigurowania dysków w RAID6 min.9:2 oraz dysk hot-spare. |  |
| 8 | Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active. |  |
| 9 | Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. |  |
| 10 | Kontrolery macierzy muszą być wyposażone w procesor wykonany w technologii wielordzeniowej. |  |
| 11 | Model oferowanej macierzy musi obsługiwać min. 140 dysków wykonanych w technologii hot-plug bez konieczności wymiany lub dodawania dodatkowych kontrolerów. |  |
| 12 | Każdy z kontrolerów macierzy musi posiadać po min 16 GB pamięci podręcznej Cache . |  |
| 13 | Zawartość pamięci Cache z danymi do zapisu na dyskach musi być identyczna dla wszystkich kontrolerów macierzy. |  |
| 14 | Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu do minimum 1600 GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności dysków SSD. |  |
| 15 | Kontrolery muszą umożliwiać ich wymianę w przypadku awarii lub planowych zadań utrzymaniowych bez konieczności wyłączania zasilania całego urządzenia. |  |
| 16 | Macierz dyskowa musi posiadać dedykowane 4 interfejsy RJ-45 Ethernet obsługujące połączenia z prędkością 100Mb/s i 1Gb/s - dla zdalnej  komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. |  |
| 17 | Każdy kontroler macierzy musi pozwalać na dołożenie interfejsów niezbędnych dla współpracy w sieci IP/FC SAN oraz NAS. |  |
| 18 | Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC, iSCSI. |  |
| 19 | Dla obsługi operacji plikowych I/O w sieci NAS Ethernet kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS przy czym obsługa protokołów CIFS i NFS musi odbywać się jednocześnie. |  |
| 20 | Dla obsługi protokołów NFS i CIFS macierz musi pozwalać na instalację minimum 4 interfejsów Ethernet 10Gb lub minimum 8 portów Ethernet 1Gb/s z portami wyprowadzonymi na kontrolerach macierzy. |  |
| 21 | Macierz musi być wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych. |  |
| 22 | Zamawiający wymaga aby macierz posiadała aktywne porty dla obsługi operacji blokowych. |  |
| 23 | Oferowana macierz musi mieć minimum 2 aktywne porty ISCSI 10Gb/s, do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, wyprowadzone na każdy kontroler RAID. |  |
| 24 | Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych: FC 16Gb/s, FC 32Gb/s, iSCSI 1 Gb/s, SAS 12Gb/s oraz porty 1/10Gb Ethernet dla dostępu plikowego. Wymiana portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu. |  |
| 25 | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1, 10, 5, 50, 6. |  |
| 26 | Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane są w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex. |  |
| 27 | Oferowana macierz musi wspierać poniższe dyski hot-plug:   * dyski elektroniczne: SSD SAS oraz SSD SAS SED. * dyski mechaniczne: HDD SAS oraz HDD NL-SAS. |  |
| 28 | Macierz musi obsługiwać dyski hot-plug SSD i HDD wyposażone w porty SAS 12Gb/s zainstalowane w dowolnym module rozwiązania. |  |
| 29 | Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”. |  |
| 30 | Macierz musi obsługiwać minimum 140 dysków SAS SSD w całym rozwiązaniu, |  |
| 31 | Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:   * dysk hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID * dysk hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID |  |
| 32 | W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk. |  |
| 33 | Macierz musi umożliwiać wyjęcie dysk hot-spare bez przebudowy skonfigurowanej wcześniej grupy dyskowej RAID. |  |
| 34 | Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit dla danych blokowych – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.  **Parametr opcjonalny dodatkowo punktowany w kryterium Parametry techniczne: TAK – 15 punktów, NIE – 0 punktów** |  |
| 35 | Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit. |  |
| 36 | Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI) jak i obsługi transmisji protokołami CIFS i NFS. |  |
| 37 | Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi odbywać się w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym, a zdalne zarządzanie macierzą odbywać się bez konieczności instalacji  żadnych dodatkowych aplikacji na stacji administratora. |  |
| 38 | Macierz musi umożliwiać wykonanie kopii migawkowych. |  |
| 39 | Macierz musi umożliwiać zdefiniowanie minimum 4000 woluminów tzw. LUN. |  |
| 40 | Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego, kontrolerów RAID i dysków bez konieczności wyłączania macierzy i bez konieczności wyłączania ścieżek logicznych iSCSI dla podłączonych serwerów. |  |
| 41 | Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupę dyskową. |  |
| 42 | Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server 2019, 2022, Oracle Linux 8, RedHat Ent Linux 8, VMWare 6.7/7.0 , Citrix XEN Server. |  |
| 43 | Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI. |  |
| 44 | Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności minimum 128TB. |  |
| 45 | Macierz musi obsługiwać Quality of Services czyli nadawanie priorytetów obsługi transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ją wraz z macierzą dla zaoferowanej pojemności macierzy. |  |
| 46 | Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Offloaded Data Transfer i Space Reclamation. |  |
| 47 | Macierz musi obsługiwać mechanizmy Thin Provisioning czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. Jeżeli taka funkcjonalność wymaga dodatkowych licencji to należy je dostarczyć wraz z macierzą dla maksymalnej pojemności dyskowej oferowanej macierzy. |  |
| 48 | Macierz musi być wyposażona w mechanizm „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Nie jest wymagane dostarczanie tej funkcjonalności, ale musi być możliwa jej rozbudowa w przyszłości. |  |
| 49 | Macierz w zaoferowanej konfiguracji musi umożliwiać uruchamianie mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych– opcja rozbudowy - Nie jest wymagane dostarczanie tej funkcjonalności, ale musi być możliwa jej rozbudowa w przyszłości. |  |
| 50 | Możliwość replikacji sprzętowej oferowanej macierzy z posiadaną przez Zamawiającego macierzą Fujitsu DX 200 S5. Nie jest wymagane dostarczanie tej funkcjonalności, ale musi być możliwa jej rozbudowa w przyszłości.  **Parametr opcjonalny dodatkowo punktowany w kryterium Parametry techniczne: TAK - 20 punktów, NIE – 0 punktów.** |  |
| 51 | Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać poziomy RAID1, RAID10, RAID5, RAID6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. |  |
| 52 | Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover) |  |
| 53 | Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). |  |
| 54 | Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawowej po usunięciu awarii macierzy podstawowej (tzw. failback). |  |
| 55 | Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. |  |
| 56 | Funkcjonalność „wysokiej dostępności” musi wspierać dwukierunkowe przełączanie macierzy podstawowej na zapasową tj. przypadek, gdy każda z tych macierzy obsługuje własne środowisko produkcyjne, a rolę jej macierzy zapasowej pełni druga z macierzy. |  |
| 57 | Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NL-SAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy |  |
| 58 | Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy |  |
| 59 | System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez protokół SNMP (wersja: 1 ,2c, 3) lub SMTP. |  |
| 60 | Całe rozwiązanie musi być objęte 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowaną wizytą technika serwisu do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. |  |
| 61 | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego. |  |
| 62 | Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat. |  |
| 63 | System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta. |  |
| 64 | Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych |  |
| 65 | Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia |  |
| 66 | Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki |  |
| 67 | Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia –**należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje**; |  |
| 68 | **Usługi**  Instalacja macierzy w szafie rack.  Podłączenie macierzy do sieci LAN oraz SAN wraz z konfiguracją stref przełączników.  Udostęnienie zasobów dyskowych na potrzeby rozbudowywanego środowiska backupu zgodnie z wytycznymi systemu Commvault Backup oraz Zamawiającego.  Dodanie macierzy do posiadanego systemu kopii zapasowych Commvault Backup.  Migracja baz deduplikacji systemu kopii zapasowych Commvault Backup.  Po procesie migracji system kopii zapasowych powinien pracować na nowo dostarczonej macierzy z zachowaniem wszystkich ustawieńi konfiguracji polityk kopii zapasowych.  Rekonfiguracja zasobów dyskowych systemu kopii zapasowych Commvault Backup.  Wyłączenie posiadanych zasobów dyskowych podłączonych do systemu kopii zapasowych Commvault Backup.  Aktualizacja systemu kopii zapasowych Commvault Backup do najnowszej dostępnej wersji.  Weryfikacja dostępności do wszystkich dotychczasowych kopii kopii zapasowych po dokonaniu migracji.  Przeprowadzenie testów środowiska. |  |

**W przypadku, gdy Wykonawca nie wpisze w poz. 17 w części dotyczącej UTM oraz poz. 34 i 50 w części dotyczącej Macierzy w Parametrach Technicznych Przedmiotu Zamówienia wymaganej informacji Zamawiający uzna, iż Wykonawca nie oferuje opcjonalnych parametrów technicznych i otrzyma 0 pkt w kryterium Parametry techniczne.**