**Załącznik nr 3.6 do SWZ**

**Opis przedmiotu zamówienia – Dostawa sprzętu i oprogramowania serwerowego wraz z montażem i uruchomieniem na potrzeby projektu „Serwer plików” zgodnie z następującymi minimalnymi parametrami technicznymi:**

**Część 6: UTM (router/firewall/IPS/VPN gateway) – wymiana sprzętu Zamawiającego w ramach programu Sonicwall Secure Upgrade – 1 sztuka**

**Oferuję (należy podać dla każdego oferowanego sprzętu z poniższych pozycji):**

Model/typ ……………………………………………………

Producent/kraj ………………………………………………

Rok produkcji (nie wcześniej niż 2023) ………………………………………………

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagania:** | **Sposób oceny** | **Parametry i warunki zaoferowane przez Wykonawcę potwierdzające wymagania Zamawiającego (należy uzupełnić wszystkie wymagane pola podając parametry oferowanego produktu lub wpisać TAK)** |
|  | Kompatybilność – 100% zgodność z systemem centralnego zarządzania urządzeniami UTM posiadanymi przez zamawiającego: Dell-Sonicwall Global Management System | TAK |  |
|  | Interfejs 10 GbE SFP+ - min. 6. | TAK, podać |  |
|  | Interfejs 1G/5G/2.5G/10G RJ45 – min.2. | TAK, podać |  |
|  | Interfejs RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa – min. 24. | TAK, podać |  |
|  | Interfejs USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G – min. 2. | TAK, podać |  |
|  | Port konsoli  | TAK |  |
|  | Interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą  | TAK |  |
|  | Urządzenie posiada dysk M.2 o pojemności przynajmniej 128 GB z możliwością wymiany na większy  | TAK |  |
|  | Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa  | TAK |  |
|  | Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji,  | TAK |  |
|  | Możliwość utworzenia przynajmniej 512 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q,  | TAK |  |
|  | Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej  | TAK |  |
|  | Ilość jednocześnie obsługiwanych połączeń: min. 4 000 000. | TAK, podać |  |
|  | Możliwość obsłużenia nowych połączeń w ciągu 1 sekundy - przynajmniej 228 000 | TAK, podać |  |
|  | Przepustowość urządzenia pracującego w trybie stateful firewall dla ramki 1518B zgodnie z RFC 2544 - 28 Gbps | TAK, podać |  |
|  | Przepustowość urządzenia pracującego z włączonym mechanizmem IPS - 17 Gbps | TAK, podać |  |
|  | Przepustowość urządzenia pracującego jako koncentrator VPN dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544 - 18 Gbps | TAK, podać |  |
|  | Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) - 16 Gbps | TAK, podać |  |
|  | Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie) - 6000 | TAK, podać |  |
|  | Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem - 2 z możliwością rozszerzenia do 1 500 | TAK, podać |  |
|  | Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem - 2 000 z możliwością rozszerzenia do przynajmniej 4 000 | TAK, podać |  |
|  | Urządzenie umożliwia poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator ma możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne  | TAK |  |
|  | Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS dla obsługi 350000 połączeń  - 7 Gbps |  |  |
|  | Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP  | TAK |  |
|  | Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)  | TAK |  |
|  | Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa)  | TAK |  |
|  | Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP  | TAK |  |
|  | Wsparcie dla Dynamicznego DNS tzw. DDNS  | TAK |  |
|  | Administrator posiada możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Muszą być dostępne takie akcje jak:  - wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),  - wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,  - wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.  | TAK |  |
|  | Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci  | TAK |  |
|  | Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego  | TAK |  |
|  | Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)  | TAK |  |
|  | Kontrola dostępności zestawionych tuneli VPN  | TAK |  |
|  | Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP  | TAK |  |
|  | Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty  | TAK |  |
|  | Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić),  | TAK |  |
|  | NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)  | TAK |  |
|  | Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych  | TAK |  |
|  | Zintegrowany system skanowania antyspyware  | TAK |  |
|  | Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www  | TAK |  |
|  | System IPS musi używać algorytmu szeregowego przetwarzania  | TAK |  |
|  | Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex)  | TAK |  |
|  | Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,  a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie. b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur, c) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.  | TAK |  |
|  | System IPS/Antywirus/Antyspyware nie posiada ograniczeń związanych z rozmiarem skanowanych plików  | TAK |  |
|  | Skanowanie IPS/Antywirus/Antyspyware jest możliwe między strefami bezpieczeństwa  | TAK |  |
|  | Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p  | TAK |  |
|  | Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń  | TAK |  |
|  | Urządzenie posiada możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji  | TAK |  |
|  | Urządzenie umożliwia analizę behawioralną (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji  | TAK |  |
|  | Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 512 takich punktów dostępowych sieci bezprzewodowej  | TAK |  |
|  | Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing - na okres 3 lat | TAK |  |
|  | Okres licencjonowania dodatkowych funkcjonalności np. świadomość i kontrola ruchu sieciowego na poziomie aplikacji, IPS, AntiMalware, Content Web filtering, itp. – min. 3 lata | TAK |  |
|  | **Gwarancja**:1. Całe rozwiązanie ma być objęte gwarancją min. 36 miesięcy - realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie w trybie min. 8 godzin przez 5 dni roboczych w tygodniu poprzez ogólnopolską linię telefoniczną producenta lub adres e-mail.
2. Usługi serwisu gwarancyjnego świadczone będą w trybie min. 8 godzin przez 5 dni roboczych w tygodniu na wszystkie elementy urządzeń (sprzęt oraz oprogramowanie), z gwarantowanym czasem skutecznej naprawy do 48 godzin.
3. Pod wskazanym numerem telefonu lub adresem e-mail można również uzyskać informacje odnośnie statusu wykonywanej/zgłoszonej naprawy.
4. Zamawiający wymaga, aby usługi serwisowe świadczone były przez producenta oferowanego sprzętu bądź autoryzowanego partnera przez cały okres gwarancji.
5. Elementy, z których zbudowane są urządzenia muszą być produktami producenta tych urządzeń lub być przez niego certyfikowane (Zamawiający może wymagać oświadczenia producenta) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne przekazane Zamawiającemu przy dostawie.
6. Jeśli naprawa nośników informacji u Zamawiającego okaże się niemożliwa, w przypadku konieczności wymiany uszkodzonych nośników informacji (zapisanych danymi Zamawiającego) na nowe wolne od wad uszkodzone nośniki pozostają u Zamawiającego.
7. W okresie gwarancji Gwarant zobowiązany jest do wykonywania, w miejscu lokalizacji przedmiotu zamówienia, następujących usług:
	* napraw uszkodzeń spowodowanych wadami technicznymi, technologicznymi i materiałowymi przy wykorzystaniu nowych nie regenerowanych, nie używanych części i podzespołów,
	* testowania poprawności działania sprzętu po wykonaniu jego naprawy,
	* telefonicznej pomocy przy rozwiązywaniu problemów dotyczących sprzętu, zwanych dalej „usługami serwisu gwarancyjnego”.
8. Wszelkie koszty naprawy w trakcie czasu trwania Gwarancji, w tym koszt transportu do serwisu, ponownej instalacji i uruchomienia ponosi Gwarant.
9. Serwis gwarancyjny musi obejmować bezpłatny dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.
10. Czas reakcji liczony od chwili zgłoszenia awarii wynosić będzie 24 godziny.
11. Czas skutecznej naprawy wad, usterek lub awarii sprzętu liczony od chwili zgłoszenia awarii do chwili usunięcia awarii potwierdzonej diagnostyką lub testem wynosić będzie 48 godziny. W przypadku, gdy podany 48 godzinny termin skutecznej naprawy wypada w dni wolne od pracy tj. sobota, niedziela lub święto termin naprawy zostanie ustalony mailowo, przy czym naprawa wykonana zostanie najpóźniej w pierwszym dniu roboczym następującym po dniu wolnym od pracy lub święcie do godziny 16.
12. Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu. Jednakże w przypadku konieczności wykonania naprawy w serwisie Producenta, Gwarant zapewni na własny koszt odbiór sprzętu do naprawy i jego dostawę po dokonaniu naprawy oraz dostarczenie sprzętu zastępczego na czas naprawy.
13. Zakres usług serwisu gwarancyjnego obejmuje również dojazd i pracę osób wykonujących czynności serwisowe w imieniu Gwaranta.
14. Każda osoba wykonująca w imieniu Wykonawcy usługi serwisu gwarancyjnego będzie posiadała dokument tożsamości i pisemne upoważnienie wystawione przez Wykonawcę oraz będzie zobligowana stosować się do przepisów wewnętrznych Zamawiającego dotyczących ruchu osobowego i materiałowego.
15. Gwarant będzie wykonywał usługi serwisu gwarancyjnego przy wykorzystaniu własnych materiałów, sprzętu i narzędzi.
16. Części lub podzespoły, które zostaną wymienione w ramach usług serwisu gwarancyjnego stają się własnością Gwaranta, który zobowiązuje się do ich bezpośredniego odbioru od Zamawiającego i utylizacji zgodnie z obowiązującymi przepisami prawa. Nie dotyczy to nośników pamięci, które pozostają u Zamawiającego.
17. W przypadku wymiany części lub podzespołów, Gwarant zobowiązany jest do dostarczenia karty gwarancyjnej (jeśli ich producent udziela odrębnej gwarancji) wraz z jej tłumaczeniem na język polski.
18. W razie nie usunięcia przez Gwaranta wad lub usterek objętych gwarancją w wyznaczonym terminie lub sprzecznie z warunkami gwarancji, Zamawiający może usunąć je na koszt Gwaranta we własnym zakresie lub zlecić ich usunięcie osobie trzeciej, z zachowaniem swoich praw wynikających z gwarancji. W przypadku skorzystania z powyższego uprawnienia Zamawiający zobowiązany jest, w formie pisemnej, do niezwłocznego powiadomienia Gwaranta o tym fakcie. Zamawiający powiadomi Gwaranta o zakresie wykonanych prac (napraw, zmian, wymiany na nowe urządzenie itp.), w takim przypadku Gwarant zobowiązany jest wypłacić Zamawiającemu kwotę stanowiącą równowartość poniesionego przez Zamawiającego kosztu wykonania tych prac.
19. W razie trzykrotnej naprawy w okresie gwarancji tego samego urządzenia, Zamawiający może żądać od Wykonawcy wymiany urządzenia na nowe, wolne od wad. W takim przypadku koszty wymiany urządzenia obciążają Gwaranta. Termin na wymianę wynosi maksymalnie 10 dni kalendarzowych od chwili zgłoszenia żądania przez Zamawiającego. W razie wymiany urządzenia na nowe, wolne od wad, termin gwarancji biegnie na nowo.
20. Udzielona gwarancja nie będzie ograniczała Zamawiającego w rozbudowie lub rekonfiguracji urządzeń o ile będą one wykonywane zgodnie z wymogami technicznymi producenta urządzeń.
21. Gwarancja nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów sprzętu. Warunki gwarancji mają pierwszeństwo przed warunkami gwarancji udzielonych przez producentów sprzętu w zakresie, w jakim warunki gwarancji przyznają Zamawiającemu silniejszą ochronę.
 | TAK, podać |  |
|  | **Inne**:1. UTM musi być fabrycznie nowa z bieżącej linii produkcyjnej (musi być obecny w ofercie na aktualnej stronie www producenta i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce. Nie dopuszcza się użycia urządzeń demonstracyjnych lub powystawowych.
2. W momencie składania oferty wszystkie elementy oferowanego urządzenia muszą być dostępne w ofercie Producenta i nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
3. UTM musi być oznakowany przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
4. Zamawiający wymaga zaktualizowania firmware półki dyskowej do najnowszej wersji kompatybilnej z wersją oprogramowania macierzy posiadaną przez Zamawiającego
5. UTM musi być dostarczony Zamawiającemu w oryginalnym opakowaniu fabrycznym.
6. Do każdego urządzenia i oprogramowania musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku angielskim lub polskim.
7. UTM musi pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
8. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.
9. Korzystanie przez Zamawiającego z dostarczonego produktu nie może naruszać majątkowych praw autorskich osób trzecich.
10. Wszystkie urządzenia muszą posiadać oznakowanie CE produktu albo spełniać normy równoważne.
11. Wszystkie urządzenia, jeśli nie podano inaczej, muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
12. Zamawiający może przed dostawą zażądać dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych.
13. Zamawiający może sprawdzić spełnienie powyższych warunków w polskim biurze producenta np. na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Gwaranta z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.
14. Dostarczany przez Dostawcę sprzęt zawiera osprzęt wymagany przez producenta oferowanego rozwiązania zgodnie z projektem technicznym (okablowanie, wkładki instalowane w dostarczanym urządzeniu, inne) niezbędny do jego prawidłowego podłączenia do infrastruktury Zamawiającego
 | TAK |  |
|  | **Dostawa**:1. Dostawca sprzętu zobowiązany jest do przestawienia scenariusza wdrożenia w podziale na daty oraz etapy do weryfikacji i zatwierdzenia przez Zamawiającego.
2. Dostawca sprzętu zobowiązany jest do instalacji i konfiguracji sprzętu w miejscu wskazanym przez Zamawiającego przy asyście pracowników Uniwersytetu Medycznego w Poznaniu.
3. Usługa instalacji i uruchomienia urządzeń musi zostać wykonana przez Producenta lub Autoryzowanego Partnera Producenta.
4. Dostawca sprzętu zobowiązany jest do dostarczenia dokumentacji powdrożeniowej zawierającej m. in. dane dostępowe.
 | TAK |  |
|  | **Dodatkowe wyposażenie:**1. Wkładki do Sonicwall, SFP+ 10 Gbit/s, wielomodowe, dwuwłóknowe – 4 szt.
2. Wkładki SFP+ 10Gbit/s wielomodowe, dwuwłóknowe do posiadanego przez Zamawiającego przełącznika DELL N4032F – 4 szt.
 | TAK |  |

*Formularz należy podpisać*

*kwalifikowanym podpisem elektronicznym*

podpisy osób/-y uprawnionych/-ej