**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**URZĄDZENIE UTM FIREWALL DO JEDNOSTEK ORGANIZACYJNYCH JST**

**URZĄDZENIE UTM FIREWALL – 3 sztuki**

(na potwierdzenie, w ramach przedmiotowych środków dowodowych należy przedstawić kartę katalogową oferowanego sprzętu)

Producent oferowanego rozwiązania: ...............................

Model oferowanego rozwiązania: ...................................

|  |
| --- |
| **Zamawiający dopuszcza zastosowanie sprzętu i oprogramowania równoważnego, poprzez który należy rozumieć sprzęt i oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co sprzęt i oprogramowanie określone w opisie przedmiotu zamówienia.** |
| **Jeżeli usunięcie awarii wymaga wymiany nośników informacji, z których nie można w sposób**  **pewny usunąć danych np. dyski, wówczas uszkodzony nośnik pozostaje w siedzibie Zamawiającego lub w jego obecności zostaje zniszczony w sposób uniemożliwiający odczytanie**  **zapisanych na nim danych** |

|  |  |
| --- | --- |
| **ARCHITEKTURA SYSTEMU** | |
| System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej | Spełnia/nie spełnia\* |
| Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. | Spełnia/nie spełnia\* |
| Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. | Spełnia/nie spełnia\* |
| Metalowa obudowa typu desktop | Spełnia/nie spełnia\* |
| Możliwość zastosowania redundantnego zasilania, z wykorzystaniem zewnętrznego zasilacza. | Spełnia/nie spełnia\* |
| Obsługa nielimitowanej ilości hostów w sieci chronionej | Spełnia/nie spełnia\* |
| Minimalna liczba i typ interfejsów fizycznych:  System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/2500  System realizujący funkcję Firewall musi dysponować minimum 1 interfejsem optycznym 1 GbE (SFP)  Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. | Spełnia/nie spełnia\* |
| Minimalna liczba nowych połączeń na sekundę: 20 000 | Spełnia/nie spełnia\* |
| Minimalna liczba jednoczesnych połączeń: 300 000 | Spełnia/nie spełnia\* |
| Minimalna przepustowość Firewall: 4 Gbps | Spełnia/nie spełnia\* |
| Minimalna przepustowość IPS: 2 Gbps | Spełnia/nie spełnia\* |
| Minimalna przepustowość Threat Protection: 500 Mbps | Spełnia/nie spełnia\* |
| Minimalna przepustowość IPSec VPN: 1 Gbps | Spełnia/nie spełnia\* |
| System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania lub musi istnieć możliwość wykorzystania karty SD do celów logowania i raportowania. | Spełnia/nie spełnia\* |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** | |
| **Zarządzanie i utrzymanie** | |
| Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. | Spełnia/nie spełnia\* |
| Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping | Spełnia/nie spełnia\* |
| Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. | Spełnia/nie spełnia\* |
| System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. | Spełnia/nie spełnia\* |
| Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego | Spełnia/nie spełnia\* |
| System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora | Spełnia/nie spełnia\* |
| System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 | Spełnia/nie spełnia\* |
| Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware) | Spełnia/nie spełnia\* |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | |
| Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia | Spełnia/nie spełnia\* |
| System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. | Spełnia/nie spełnia\* |
| Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. | Spełnia/nie spełnia\* |
| System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). | Spełnia/nie spełnia\* |
| System musi zapewniać ochronę przed skanowaniem portów (portscan blocking). | Spełnia/nie spełnia\* |
| System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać obsługę routingu statycznego | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. | Spełnia/nie spełnia\* |
| System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. | Spełnia/nie spełnia\* |
| System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. | Spełnia/nie spełnia\* |
| Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe | Spełnia/nie spełnia\* |
| Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. | Spełnia/nie spełnia\* |
| W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). | Spełnia/nie spełnia\* |
| Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.  Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. | Spełnia/nie spełnia\* |
| System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover | Spełnia/nie spełnia\* |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | |
| System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia | Spełnia/nie spełnia\* |
| System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. | Spełnia/nie spełnia\* |
| **Autoryzacja użytkowników** | |
| Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont | Spełnia/nie spełnia\* |
| System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. | Spełnia/nie spełnia\* |
| Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). | Spełnia/nie spełnia\* |
| Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. | Spełnia/nie spełnia\* |
| **Samoobsługowy portal dla użytkowników** | |
| Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). | Spełnia/nie spełnia\* |
| Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android  Rozwiązanie musi umożliwiać zmianę hasła. | Spełnia/nie spełnia\* |
| **Podstawowe opcje VPN** | |
| System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: | Spełnia/nie spełnia\* |
| Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) | Spełnia/nie spełnia\* |
| Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika). | Spełnia/nie spełnia\* |
| **OCHRONA SIECI** | |
| **IPS** | |
| Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS | Spełnia/nie spełnia\* |
| Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur | Spełnia/nie spełnia\* |
| System musi generować alerty w przypadku wykrycia ataku. | Spełnia/nie spełnia\* |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** | |
| **Ochrona i kontrola Web** | |
| Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. | Spełnia/nie spełnia\* |
| System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.  System musi filtrować pliki na podstawie MIME | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. | Spełnia/nie spełnia\* |
| Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS | Spełnia/nie spełnia\* |
| System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego | Spełnia/nie spełnia\* |
| **Ochrona i kontrola aplikacji** | |
| Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) | Spełnia/nie spełnia\* |
| Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania | Spełnia/nie spełnia\* |
| **Kształtowanie pasma dla Web i Aplikacji** | |
| Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym. | Spełnia/nie spełnia\* |
| **OCHRONA ANTYWIRUSOWA** | |
| **Ochrona i kontrola Email** | |
| Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy | Spełnia/nie spełnia\* |
| System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń | Spełnia/nie spełnia\* |
| System musi zapewniać wykrywanie, blokowanie i skanowanie załączników | Spełnia/nie spełnia\* |
| Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. | Spełnia/nie spełnia\* |
| Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka. | Spełnia/nie spełnia\* |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** | |
| **On-cloud Sandboxing** | |
| Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. | Spełnia/nie spełnia\* |
| Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab | Spełnia/nie spełnia\* |
| System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows . | Spełnia/nie spełnia\* |
| **LOGOWANIE I RAPORTOWANIE** | |
| System musi umożliwiać składowanie oraz archiwizację logów. | Spełnia/nie spełnia\* |
| System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. | Spełnia/nie spełnia\* |
| System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących | Spełnia/nie spełnia\* |
| System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). | Spełnia/nie spełnia\* |
| Rozwiązanie musi generować raporty w HTML i CSV | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog | Spełnia/nie spełnia\* |
| System musi zapewniać podgląd wykorzystania łącza internetowego | Spełnia/nie spełnia\* |
| System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP | Spełnia/nie spełnia\* |
| Rozwiązanie musi oferować możliwość zanonimizowania danych | Spełnia/nie spełnia\* |
| **POZOSTAŁE** | |
| **Certyfikaty** | |
| Urządzenie musi posiadać:  - certyfikat Common Criteria;  - certyfikat ICSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE; | Spełnia/nie spełnia\* |
| **GWARANCJA I SERWIS** | |
| Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, kanału dystrybucji. | Spełnia/nie spełnia\* |
| Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na terenie UE – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. Brokerki, | Spełnia/nie spełnia\* |
| Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu, | Spełnia/nie spełnia\* |
| Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta, | Spełnia/nie spełnia\* |
| Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych. | Spełnia/nie spełnia\* |
| Na dostarczany sprzęt musi być udzielona **min. 60-miesięczna gwarancja**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań, | Spełnia/nie spełnia\* |
| Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę), | Spełnia/nie spełnia\* |
| bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji, | Spełnia/nie spełnia\* |
| dostęp do dokumentacji sprzętu i oprogramowania, | Spełnia/nie spełnia\* |
| dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej, | Spełnia/nie spełnia\* |
| dostęp do pomocy technicznej producenta. | Spełnia/nie spełnia\* |
| licencje obejmujące wszystkie wymagane moduły na okres **min. 24 miesięce** | Spełnia/nie spełnia\* |
| możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji. | Spełnia/nie spełnia\* |

\*nie potrzebne skreślić

Cena netto zaoferowanego produktu (Urządzenie UTM Firewall) – 3 sztuki:

…………………………………………………………………………………………

Cena brutto zaoferowanego produktu (Urządzenie UTM Firewall) – 3 sztuki:

…………………………………………………………………………………………

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**USŁUGA WDROŻENIA URZĄDZEŃ UTM FIREWALL I KONFIGURACJI SZYFROWANEGO POŁĄCZENIA IPSec VPN W LOKALIZACJACH JEDNOSTEK ORGANIZACYJNYCH JST WSKAZANYCH PRZEZ ZAMAWIAJĄCEGO ORAZ W SIEDZIBIE ZAMAWIAJĄCEGO**

**Usługa wdrożenia urządzeń UTM w trzech lokalizacjach wskazanych przez Zamawiającego oraz usługa konfiguracji szyfrowanego połączenia IPSec VPN z siedzibą Zamawiającego, w trzech lokalizacjach wskazanych przez Zamawiającego oraz w siedzibie Zamawiającego**

|  |  |
| --- | --- |
| **Minimalne wymagania wdrożenia i konfiguracji zgodnie z wymaganiami klienta** | |
| Konfiguracja sieci (interfejsy i routing) | Spełnia/nie spełnia\* |
| Konfiguracja firewalla | Spełnia/nie spełnia\* |
| Konfiguracja NAT | Spełnia/nie spełnia\* |
| Konfiguracja IPS | Spełnia/nie spełnia\* |
| Konfiguracja dodatkowych usług sieciowych tj. DHCP |  |
| Konfiguracja urządzenia do współpracy z dostawcą Internetu (dostęp do Internetu) | Spełnia/nie spełnia\* |
| Integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników) | Spełnia/nie spełnia\* |
| Transparentna autoryzacja w Active Directory – instruktaż przebiegu  instalacji | Spełnia/nie spełnia\* |
| Konfiguracja połączenia VPN IPSec Site-to-Site trzech lokalizacji wskazanych przez Zamawiającego z siedzibą Zamawiającego (wymagana konfiguracja IPSec VPN również w siedzibie Zamawiającego w Ochotnicy Dolnej na urządzeniu klasy UTM Firewall marki Stormshield model SN510) | Spełnia/nie spełnia\* |
| Konfiguracja połączenia VPN Client-to-Site na pojedynczej, wzorcowej stacji roboczej Zamawiającego (instruktaż konfiguracji) | Spełnia/nie spełnia\* |
| Usługi musi zostać zrealizowana przez wdrożeniowca autoryzowanago przez producenta lub autoryzowanego dystrybutora dostarczanego rozwiązania sprzętowego klasy UTM | Spełnia/nie spełnia\* |
| Zamawiający dopuszcza możliwość wykonania usługi w trybie zdalnym pod warunkiem, że dostarczone rozwiązanie klasy UTM pozwala na taką możliwość (bezpośredni dostęp zdalny do urządzenia klasy UTM udostępniony wg. dostarczonej instrukcji producenta oferowanego rozwiązania wraz z instrukcją wstępnej konfiguracji dostępu do sieci internetowej).  Urządzenie konfigurowane w ramach usługi wykonywanej w ten sposób zostanie podłączone do odizolowanej od sieci produkcyjnej sieci internetowej. Zamawiający po wykonaniu usługi przez Wykonawcę zastąpi nadaną adresację sieci urządzenia adresami sieci produkcyjnej. | Spełnia/nie spełnia\* |

\*niepotrzebne skreślić

Cena netto wykonania usługi:

…………………………………………………………………………………………

Cena brutto wykonania usługi:

…………………………………………………………………………………………

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

Podpis osoby - osób upoważnionych do składania

oświadczeń woli w imieniu wykonawcy