**Załącznik nr 1 G do FORMULARZA OFERTOWEGO**

**Parametry techniczne i wyposażenie**

**CZĘŚĆ VII – Urządzenie klasy utm**

WYPEŁNIA WYKONAWCA:

Dane Wykonawcy (nazwa, adres) : …………………………………………………………………………………….

Oferuję dostawę urządzenia klasy UTM PRODUCENTA: ………………….…………………

MARKA/MODEL/TYP/OZNACZENIE HANDLOWE: ……………………………………………………………..

UWAGA:

Kolumny nr 3 pt. „Potwierdzenie spełnienia wymagań TAK/NIE” należy wypełnić stosując słowa TAK lub NIE.

W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „NIE” lub zaoferuje niższe wartości niż wymagane, oferta zostanie odrzucona, jako że jej treść jest niezgodna z warunkami zamówienia (art. 226 ust. 1 pkt 5 ustawy Pzp).

**„Dostawa urządzeń i oprogramowania wraz z  przeprowadzeniem audytu cyberbezpieczeństwa wraz ze szkoleniami dla pracowników z zakresu cyberbezpieczeństwa w ramach realizacji projektu Cyfrowa Gmina przez Gminę Ząbkowice Śląskie” z podziałem na 9 zadań/ części. ”**

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostawy przedmiotu zamówienia wraz z jego rozpakowaniem, sprawdzeniem poprawności działania i ustawieniem w wyznaczonym przez Zamawiającego pomieszczeniu na terenie Urzędu.

Wykonawca zobowiązany do utylizacji na własny koszt wszelkich niepotrzebnych materiałów zabezpieczających urządzenia podczas transportu, w tym kartony, folie, taśmy klejące etc.

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.

Potwierdzenie spełniania poniższych, minimalnych warunków:

| Zakres wymagania | Wymaganie / Dokument | Potwierdzenie spełnienia wymagań  TAK/NIE |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** | |
| **Typ** | Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami oraz wdrożeniem i szkoleniem | **[….]** |
| **Wymagania techniczne** | * + - 1. Zapora sieciowa typu Next Generation Firewall (NGFW),       2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.       3. Minimalna ilość interfejsów:   a) 6 interfejsów 10 GbE SFP+,   * 1. 4 interfejsy 5 GbE SFP+,   2. 24 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.   3. 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,   4. 1 interfejs konsoli do zarządzania zaporą,   5. 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą,  1. Zapora powinna posiadać dysk M.2 o pojemności przynajmniej 128 GB z możliwością wymiany na większy. 2. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa 3. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji, 4. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q, 5. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej, 6. Minimalna ilość jednocześnie obsługiwanych połączeń: 2 000 000, 7. Możliwość obsłużenia przynajmniej 22 500 nowych połączeń w ciągu 1 sekundy. 8. Przepustowość urządzenia pracującego w trybie stateful firewall: 5,5 Gbps – dla ramki 1518B zgodnie z RFC 2544, 9. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 3.8 Gbps, 10. Przepustowość urządzenia pracującego jako koncentrator VPN: 2,2 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544, 11. 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) – 3,5 Gbps, 12. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3 000, 13. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 500 14. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000. 15. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne. 16. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 850 Mbps oraz obsłużyć 150 000 połączeń. 17. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, 18. 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), 19. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa), 20. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, 21. Wsparcie dla Dynamicznego DNS tzw. DDNS, 22. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne. 23. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony, na które użytkownik wchodzi bezpośrednio). 24. Administrator powinien mieć możliwość tworzenia różnych akcji, dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:     1. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),     2. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,     3. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. 25. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps, 26. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL. 27. 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. 28. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. 29. 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), 30. Kontrola dostępności zestawionych tuneli VPN, 31. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. 32. 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. 33. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić) 34. Funkcja NAT oparta o reguły bezpieczeństwa. 35. 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), 36. 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. 37. Zintegrowany system skanowania antyspyware, 38. 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. 39. System IPS musi używać algorytmu szeregowego przetwarzania. 40. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex). 41. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,     1. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.     2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,     3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur. 42. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików. 43. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa, 44. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi, 45. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p, 46. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, 47. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji. 48. Urządzenie powinno mieć możliwość analizy behawioralnej (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. 49. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej. | **[….]** |
| **Gwarancja** | Min. 24 miesiące wraz ze wsparciem technicznym w trybie 24x7. | **[….]** |
| **Wymagania licencyjne** | Wraz z urządzeniem Zamawiający wymaga dostarczenia subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat.  Dodatkowe Zamawiający wymaga, aby posiadane aktywne subskrypcje na obecnie posiadanym urządzeniu SONICWALL ADVANCED GATEWAY SECURITY SUITE BUNDLE FOR NSA 2600 ważne do dnia 16.04.2023 zostały przeniesione i dodane do subskrypcji oferowanego urządzenia. | **[….]** |
| **Wymagania dodatkowe** | W ramach dostawy Wykonawca zobowiązany jest do przeprowadzenia:  1) Wdrożenie  -Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, konfiguracja routingu, DNS, NTP),  -Konfiguracja profilów administracyjnych,  Podpięcie weryfikacja statusu licencji,  -Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy),  -Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa,  -Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa,  -Konfiguracja lokalnej bazy użytkowników oraz zdefiniowanie grup, oraz podłączenie do usługi LDAP/AD  Konfiguracja VPN wg potrzeby  -Konfiguracja IPSec VPN site-to-site,  --Konfiguracja IPSec VPN client-to-site,  -Konfiguracja SSL VPN client-to-site,  -Konfiguracja profilów kontroli Antywirusowej i podpięcie do polityk FW,  -Konfiguracja profilów ochrony przed atakami IPS i podpięcie do polityk FW,  -Konfiguracja profilów kontroli aplikacji i podpięcie do polityk FW,  -Konfiguracja profilów kontroli WWW i podpięcie do polityk FW,  -Konfiguracja profilów antyspamowych i podpięcie do polityk FW,  -Test zastosowanych funkcji ochronnych,  -Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji.  2) Instruktaż zdalny  Wymagane jest, aby wdrożenie oraz instruktaż został wykonany przez inżynierów certyfikowanych przez producenta dostarczonego rozwiązania klasy UTM (do oferty dołączyć certyfikaty inżynierów) w minimalnym zakresie:  -Przeszkolenie z zakresu zarządzania wszystkimi elementami podlegającymi konfiguracji w punkcie “Wdrożenie”  -Szkolenie musi trwać minimum 3h  -Szkolenie z odtwarzania konfiguracji po awarii urządzenia backup lokalny/backup z chmury producenta.  -Szkolenie dotyczące generowania logów  -Szkolenie dotyczące konfiguracji tuneli VPN w tym SSL VPN/IPSEC  -Przeszkolenie z zakresu prostych narzędzi do rozwiązywania problemów. | **[….]** |
| **Ilość** | 1 szt. | **[….]** |

............................, dn. \_ \_ . \_ \_ . \_ \_ \_ \_r.

**KWALIFIKOWANY PODPIS ELEKTRONICZNY Wykonawcy**

**lub osób uprawnionych do składania oświadczeń**

**woli w imieniu Wykonawcy**