Załącznik nr 1 do SIWZ

Opis Przedmiotu Zamówienia do SIWZ

I. Opis przedmiotu zamówienia w postępowaniu na dostawę urządzenia UTM na potrzeby Starostwa Powiatowego w Rykach znak sprawy OR.272.6.2020

1. Wykonawca zobowiązany jest dostarczyć sprzęt i oprogramowanie o parametrach zgodnych lub lepszych z wymaganiami przedstawionymi w niniejszym rozdziale.

Zamawiający wymaga aby:

a.sprzęt był fabrycznie nowy i nieużywany, z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy,

b.korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich,

c.sprzęt, na dzień składania oferty przez Wykonawcę, nie był przeznaczony przez producenta tego sprzętu do wycofania z produkcji lub sprzedaży w okresie minimum 6 miesięcy od dnia składania ofert,

d.korzystanie przez Zamawiającego ze sprzętu, oprogramowania układowego tego sprzętu lub innych podzespołów i licencji oprogramowania serwerowego będącego przedmiotem zamówienia nie naruszało majątkowych praw autorskich osób trzecich.

Zamawiający zastrzega sobie prawo do:

- zwrócenia się do producenta oferowanego sprzętu o potwierdzenie ich zgodności z zamówieniem,
- zlecenia producentowi oferowanego sprzętu, lub wskazanemu przez producenta podmiotowi, inspekcji sprzętu pod kątem ich zgodności z zamówieniem oraz ważności i zakresu uprawnień licencyjnych.

W przypadku stwierdzenia niezgodności sprzętu z ofertą Wykonawcy, Zamawiający zwróci niezgodny sprzęt na koszt Wykonawcy. Jednocześnie Wykonawca zostanie obciążony kosztami za inspekcję sprzętu pod kątem ich zgodności z zamówieniem oraz ważności i zakresu uprawnień licencyjnych przez podmiot je wykonujący, w przypadku gdy Zamawiający skorzysta z prawa do wykonania takiej inspekcji.

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest:

a)dostarczyć na własny koszt i ryzyko sprzęt wskazany w ofercie do siedziby Zamawiającego.

b) przeprowadzić wdrożenie dostarczonego urządzenia UTM zastępując nim obecnie pracujące urządzenie UTM Zamawiającego (Stormshild SN500), przeprowadzić szkolenie dla administratora IT Zamawiającego z konfiguracji urządzenia z zakresu wdrożenia.

II. Szczegółowy opis przedmiotu zamówienia:

ARCHITEKTURA	Dostarczony system bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje bezpieczeństwa.
FUNKCJONALNOŚCI	-Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. -Klaster Active-Passive każdego z elementów systemu. -Elementy systemu przenoszące ruch użytkowników w jednym z dwóch trybów: Router/NAT lub transparent. -System realizujący funkcję Firewall z 12 interfejsami miedzianymi Ethernet 10/100/1000.

	-Możliwość tworzenia 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. -W zakresie Firewall'a obsługa 500 tys jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę. -System realizujący funkcję Firewall wyposażony w lokalny dysk o pojemności 200 GB do celów logowania i raportowania. -Wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. -System ochrony realizowany za pomocą funkcjonalności. a)Kontrola dostępu - zapora ogniowa klasy Stateful Inspection b)Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV skanuje pliki typu: rar, zip. c)Poufność danych - IPSec VPN oraz SSL VPN d)Ochrona przed atakami - Intrusion Prevention System [IPS/IDS] e)Kontrola stron Internetowych – Web Filter [WF] f)Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3) g)Kontrola pasma oraz ruchu [QoS i Traffic shaping] h)Kontrola aplikacji oraz rozpoznawanie ruchu P2P i)Analiza ruchu szyfrowanego protokołem SSL -Wydajność systemu Firewall 8 Gbps -Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus 950 Mbps -Wydajność ochrony przed atakami (IPS) 3,3 Gbps -Wydajność VPN IPSec 1,3 Gbps -Funkcjonalności VPN: a)Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site b)Dołączony bezpłatny klient VPN na 100 użytkowników c)Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności d)Praca w topologii Hub and Spoke oraz Mesh e)Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth f)Obsługa ssl vpn w trybach portal oraz tunel -Rozwiązanie zapewnia: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. -Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. -Polityka bezpieczeństwa systemu zabezpieczeń uwzględnia adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety). -Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. -Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). -Ochrona IPS opiera się na analizie protokołów i sygnatur. Baza wykrywanych ataków zawiera 1000 wpisów. Wykrywanie anomalii protokołów i ruchu stanowiące podstawową ochronę przed atakami typu DoS oraz DDos. -Funkcja kontroli aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. -Baza filtra WWW pogrupowana w 50 kategorii tematycznych. W ramach filtra www są dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. -Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych

	oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. -System zabezpieczeń umożliwia wykonywanie uwierzytelniania tożsamości użytkowników za pomocą: a)Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu b)Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP c)Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych d)Rozwiązanie umożliwia budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny -System raportowania i przeglądania logów: a)Predefiniowane raporty dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego b)Generowanie 25 różnych typów raportów -System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie wymaga dodatkowej licencji do swojego działania -Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall posiada certyfikat EAL4+ dla rozwiązań kategorii Network Firewall. -Elementy systemu mają możliwość zarządzania lokalnego (HTTPS, SSH) oraz współpracują z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
SERWISY I LICENCJE	W ramach zamówienia Wykonawca dostarczy licencje aktywacyjne dla wszystkich wymienionych funkcjonalności, uprawniające do używania ww. funkcji oraz pobierania aktualizacji baz zabezpieczeń minimum w na okres 1 roku lub przeniesie obecnie posiadaną przez zamawiającego licencje (ważność do 26.09.2021) UTM Security Pack Strosmshild na nowe urządzenie.
GWARANCJA	Gwarancja na bazie świadczenia gwarancyjnego producenta sprzętu przez okres minimum 12 miesięcy. Wykonawca zapewnia, że dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji producenta sprzętu. Z dostawą sprzętu Wykonawca zobowiązuje się dostarczyć dokument wydany przez producenta lub jego polskiego przedstawiciela, potwierdzający że sprzęt jest nowy (potwierdzająca data produkcji), pochodzi z oficjalnego kanału dystrybucji, pochodzi z bieżącej produkcji i objęty jest wsparciem serwisowym producenta .
INNE	-Dostarczony sprzęt musi być fabrycznie nowy i oryginalnie zapakowany. -Wykonawca przeprowadzi wdrożenie dostarczonego urządzenia UTM zastępując nim obecnie pracujące urządzenie UTM Zamawiającego (Stormshild SN500). Konfiguracja obecnego urządzenia UTM składa się z następujących elementów: -56 –polityk 220 -obiektów adresowych firewalla -1 –tunel VPNRouting –tylko statyczny, -Wykonawca przeprowadzi szkolenie dla administratora IT Zamawiającego z konfiguracji urządzenia z zakresu wdrożenia.