Załącznik Nr 1

Pak Nr 1

Dostawa urządzenia sieciowego UTM.

1. Przedmiot zamówienia:

Przedmiotem zamówienia jest dostawa urządzenia sieciowego UTM (1 szt.) wraz z jego instalacją i konfiguracją. Wyznaczony przez Wykonawcę inżynier posiadający certyfikat producenta urządzenia przeprowadzi w trakcie wdrażania szkolenie dla dwóch pracowników w zakresie podstawowej obsługi urządzenia. Wykonawca powinien przeprowadzić dodatkowe jedniodniowe szkolenie z zakresu konfiguracji i administracji sprzętu. Uczestnicy szkolenia otrzymają certyfikat od Wykonawcy potwierdzający zdobytą wiedzę w/w zakresach. Etap wdrażania i szkolenia nie powinien przekroczyć 3 dni roboczych.

2. Opis przedmiotu zamówienia:

Parametry techniczne sprzętu wskazanego przez Zamawiającego są parametrami minimalnymi. Zamawiający dopuszcza dostawę produktów równoważnych, w stosunku do zawartych w opisie przedmiotu zamówienia. W celu potwierdzenia, że oferowane dostawy odpowiadają wymaganiom określonym przez Zamawiającego, Wykonawca zobowiązany jest dołączyć do oferty opis urządzenia technicznego (karta katalogowa produktu) potwierdzającego, że oferowany produkt jest równoważny w określonych parametrach.

Urządzenie sieciowe typu UTM – ilość 1 szt.

Producent / kraj pochodzenia:

Nazwa / typ:

Rok produkcji: fabrycznie nowe wyprodukowane nie wcześniej niż 2015 lub 2016

Wykonawca / adres siedziby:

Lp.	Nazwa parametru	Wymagania minimalne Parametry techniczne	PARAMETRY OFEROWANE
1.	**Ilość i rodzaj interfejsów:**	• 10/100/1000 (RJ-45) - 22 (2 x WAN, 1 x DMZ, 1 x Management, 2 x High Availbility, 16 x LAN), • USB - 1 (klient)/ 2(Serwer).	
2.	**Pamięć wewnętrzna:**	Lokalny dysk o pojemności min. 16 Gb do celów logowania i raportowania.	
3.	**Architektura systemu ochrony:**	Wszystkie dostępne funkcje ochronne oraz zastosowane technologie a także system operacyjny muszą pochodzić od jednego producenta.	
4.	**System operacyjny:**	Dedykowany system operacyjny producenta urządzenia.	
5.	**Funkcjonalności:**	Najważniejsze funkcje: Firewall: • NAT, PAT oraz Bridge, (Translacja adresów NAT adresu źródłowego i NAT adresu docelowego). • Policy-Based NAT, SIP/H.323/SCCP NAT Traversal, • VLAN Tagging (802.1Q), min 254 interfejsy • Wsparcie dla protokołu IPv6,	

		IPS: • Automatyczna aktualizacja bazy danych, • Sensor IPS, DoS, • Wsparcie dla protokołu IPv6, Antywirus/Antyspyware: • Automatyczna aktualizacja, • Proxy-Based Antywirus, • Proxy-Flow Antywirus, • Kwarantanna, • Wsparcie dla protokołu IPv6, VPN: • IPSec, SSL VPN, • Autentyfikacja DES, 3DES, AES, SHA-1/MD5, • PPTP, L2TP, VPN Client Pass Through, • SSL Single Sign-On Boomarks, • Two-Factor Authentication, WAN • Optymalizacja Gateway-Gateway, • Dwukierunkowa optymalizacja Gateway-Client, • Buforowanie WEB, • Bezpieczne tunele, • Tryb transparentny, Inspekcja ruchu SSL • Protokoły: HTTPS, SMTPS, POP3S, IMAPS, • Inspekcja: Antivirus, Web Filtering, Antispam, Data Loss Prevention, • SSL Offload, DLP • Identyfikacja oraz kontrola danych w ruchu, • Wbudowana baza wzorców, • Kontrola formatu plików, • Wsparcie dla symboli między narodowych, Kontrola aplikacji • Identyfikacji oraz kontrola aplikacji, • Kształtowanie ruchu, • Kontrola aplikacji bez względu na port oraz protokół (np. Facebook, BiTorrent, Skype, eDonkey, MSN, KaZaa), Wirtualne domeny: • Wydzielony Firewall/Domeny routingu, • Oddzielne domeny administracyjne, • Oddzielne interfejsy VLAN,	
6.	**Dodatkowe**	• Rozwiązanie powinno zapewniać: obsługę Policy	

	funkcjonalności	Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN. • Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a. • Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety) • Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) • Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. • Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP • Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. • Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	
7.	**Połączenia VPN**	W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:	

		• Tworzenie połączeń w topologii Site-to-site oraz Client-to-site • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Praca w topologii Hub and Spoke oraz Mesh • Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	
8.	**Uwierzytelnianie użytkowników:**	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • 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 • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.	
9.	**Wydajność:**	• Przepustowość Firewall: • nie mniej niż 2500 Mbps dla pak 1518 byte UDP • nie mniej niż 1000 Mbps dla pak 512 byte UDP • nie mniej niż 200 Mbps dla pak 64 byte UDP • Ilość jednoczesnych sesji – nie mniej niż 2 Miliony, • Ilość nowych sesji – nie mniej niż 20,000, • Przepustowość IPSec VPN – nie mniej niż 400 Mbps, • Przepustowość IPS – nie mniej niż 500 Mbps, • Ilość tuneli IPSec VPN (Gateway-Gateway) – nie mniej niż 1,500, • Ilość tuneli IPSec VPN (Client-Gateway) – nie mnie niż 5,000, • Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączoną funkcją: Antivirus min. 300 Mbps • Wirualne domeny – nie mniej niż 10.	
10.	**Funkcjonalność zapewniająca niezawodność (High Availbility):**	Monitorowanie i wykrywanie uszkodzenia elementów sprzętowych i oprogramowania systemu zabezpieczeń oraz połączeń sieciowych. Połączenie dwóch identycznych urządzeń w klaster: Tryby pracy: • Active – Active, • Active – Passive.	

11.	**Konfiguracja i zarządzanie:**	Konfiguracja poprzez terminal, linię komend a także GUI. Dostęp do urządzenia musi być szyfrowany. Zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. System powinien umożliwiać aktualizację oprogramowania oraz zapisanie konfiguracji o odtworzenie z pamięci USB.	
12.	**Raportowanie:**	Urządzenie powinno mieć możliwość współpracy z zewnętrznym (sprzętowym) modułem raportowania: zbieranie logów z urządzeń, generowanie raportów.	
13.	**Certyfikaty:**	• ICSA Labs dla funkcjonalności: IPSec, IPS, Antivirus, SSL VPN. • ICSA lub EAL4 dla funkcjonalności Firewall	
14.	**Serwis i licencje (subksrybcje):**	Dostawca dostarczy licencje aktywacyjne, aktualizacje wszystkich modułów urządzenia (tzn. FIREWALL, IPS, WEB FILTERING, obsługa kanałów VPN, ochrona Antyspam i Antywirus), wsparcie techniczne producenta dystrybucji oraz dostawcy na okres nie krótszy 60 miesięcy .	
15.	**Gwarancja:**	System powinien być objęty serwisem gwarancyjnym producenta przez okres minimum 60 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. Warunki gwarancji wraz z kartą gwarancyjną należy załączyć do sprzętu w wersji papierowej.	
16.	**Instalacja i konfiguracja:**	Instalacja i konfiguracja urządzenia powinna być przeprowadzona w obecności wyznaczonych przez Zamawiającego pracowników, przeprowadzona na miejscu w siedzibie Zamawiającego. Wyznaczony przez Wykonawcę inżynier posiadający certyfikat producenta urządzenia przeprowadzi w trakcie wdrażania szkolenie dla dwóch pracowników w zakresie podstawowej obsługi urządzenia. Wykonawca powinien przeprowadzić dodatkowe, jednodniowe szkolenie z zakresu konfiguracji i administracji sprzętu. Uczestnicy szkolenia otrzymają certyfikat od Wykonawcy potwierdzający zdobytą wiedzę w/w zakresach.	

Wykaz osób, które będą wykonywać zamówienie lub będą uczestniczyć w wykonywaniu zamówienia

Lp.	Imię i Nazwisko	Kwalifikacje (dotyczące zamówienia)	Zakres wykonywanych czynności
1.			
2.			

Na potwierdzenie kwalifikacji osoby lub osób wykonujących przedmiot zamówienia Wykonawca zobowiązany jest dołączyć certyfikaty producenta potwierdza kwalifikacje inżynierów.

Nie spełnienie choć jednego parametru spowoduje odrzucenie oferty.

Niniejszym oświadczamy, że w/w urządzenia są kompletne i w pełni gotowe do pracy i nie wymagane są żadne dodatkowe zakupy. Do oferty należy dołączyć komplet oryginalnych materiałów informacyjnych producenta potwierdzających spełnienie żądanych wymagań.

W cenę wykonawca wlicza również subskrypcje licencji, które muszą zapewnić sprawna pracę w/w urządzenia dla wszystkich modułów, aktualizowane w trakcie obowiązywania umowy.

Ogółem wartość netto …….

Podatek VAT % …….

Ogółem wartość brutto …….

.....

(podpis i pieczątka uprawnionego przedstawiciela firmy/ Wykonawca