Mszanowo 22.03.2019 r.

RI.271.1.9.2019.ZP

Wykonawcy

dotyczy: przetargu nieograniczonego na ***„Dostawę sprzętu w ramach projektu: Wyrównywanie szans edukacyjnych uczniów w Gminie Nowe Miasto Lubawskie" - III***

Ogłoszenie o zamówieniu **525514-N-2019 z dnia 2019-03-14.**
Ogłoszenie o zmianie ogłoszenia **540053193-N-2019 z dnia 20-03-2019 r.**

Na podstawie art. 38 ust.2 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2018 r. poz. 1986 ze zm.), w związku z pytaniami i uwagami do udzielonej odpowiedzi dotyczącej routera jakie wpłynęły do Zamawiającego, Zamawiający ponownie zmienia opis routera :

Pytanie nr 1
„Niniejszym zgłaszamy naszą uwagę Państwu do opublikowanej odpowiedź NR 2 na nasze pytanie dotyczące tendencyjności w opisie routera i wskazaniu konkretnego producenta oraz modelu urządzenia. Przedstawiona w odpowiedzi nr 2 specyfikacja to tylko rozbudowa jeszcze bardziej postać opisu tego co było pierwotnie. Jednoznacznie możemy stwierdzić, że wymagania określone teraz dla routera spełnia cały czas tylko jeden producent. To, że zniknęły nazwy własne, wcale nie potwierdza tego, że teraz wymagania spełniają jeszcze inni producenci. Tak na pewno nie jest i jedynym producentem jest nadal Fortinet z urządzeniem FG-30E."

Odpowiedź:
W załączniku nr 6 do SIWZ – opisie przedmiotu zamówienia poz. 5 „Router" Zamawiający w całości zmienia opis przedmiotu zamówienia, w ten sposób, że zastępuje dotychczasowy opis na następujący:
Dostarczony system bezpieczeństwa musi posiadać wydajność dedykowaną przez producenta na poziomie umożliwiającym obsługę sieci lokalnej posiadającej 30 komputerów. Musi posiadać panel zarządzający w języku polskim, dostępny przez przeglądarkę internetową. Musi ponadto zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Dla elementów systemu bezpieczeństwa musi zapewnić wszystkie poniższe funkcjonalności:
1) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2) Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
3) System realizujący funkcję Firewall musi dysponować minimum 5 interfejsami miedzianymi Ethernet 10/100/1000 (w tym min. jeden interfejs WAN), 1 portem konsoli RJ45, 1 portem USB

4) Możliwość tworzenia minimum 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
5) W zakresie Firewall'a obsługa nie mniej niż 150 tys. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.
6) System realizujący funkcję Firewall musi posiadać system raportowania i przeglądania logów zebranych na urządzeniu.
7) W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności: Kontrola dostępu - zapora ogniowa klasy Stateful Inspection, Ochrona przed wirusami – antywirus, Poufność danych - obsługa IPSec VPN oraz SSL VPN, Ochrona przed atakami - Intrusion Prevention System, Kontrola stron Internetowych – Web Filter, Kontrola zawartości poczty – antyspam, Kontrola pasma oraz ruchu QoS i Traffic shaping, Kontrola aplikacji oraz rozpoznawanie ruchu P2P, Analiza ruchu szyfrowanego protokołem SSL
8) W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site, Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem, Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności , Obsługa ssl vpn w trybach portal oraz tunel
9) Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
10) Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
11) 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).
12) Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
13) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
14) Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
15) Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
16) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
17) Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
18) 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) w oparciu o zewnętrzne bazy danych, Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.
19) System zabezpieczeń musi umożliwiać w zakresie realizowanych funkcjonalności raportowanie i przeglądania logów

20) Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4 + dla rozwiązań kategorii Network Firewall.
21) Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Pytanie nr 2
Zamawiający podał w SIWZ następujący wymóg: „Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 64bit", Microsoft już nie prowadzi certyfikacji WHCL, poświadczającej zgodność oferowanego sprzętu komputerowego z ich oprogramowaniem. Producent aktualnie osobiście przeprowadza testy zgodności i umieszcza informację o zgodności z systemem operacyjnym np. na opakowaniu, w instrukcji obsługi. Certyfikaty WHCL już od jakiegoś czasu nie są wydawane i publikowane na stronie Microsoftu, więc na wszystkie nowsze konfiguracje producenci sprzętu komputerowego takiego certyfikatu nie posiadają i nie mają możliwości go przekazać przy dostawach. Dlatego zwracamy się o usunięcie wymienionego zapisu bądź dodanie „certyfikat lub oświadczenie producenta komputerów.

Odpowiedź:
W załączniku nr 6 do SIWZ – opisie przedmiotu zamówienia w poz. 1 „Zestaw komputerowy stacjonarny" oraz poz. 8 „Laptop z oprogramowaniem" - Zamawiający zmienia zapis „Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 64bit" **na** „Oferowane modele komputerów muszą być w pełni kompatybilne z systemem Windows 10 64bit, co należy wykazać certyfikatem Microsoft lub certyfikatem/oświadczeniem producenta komputera.

Pytanie nr 3
Pozycja 7. Słuchawki
Przeznaczenie słuchawek - do jakich urządzeń mają być podłączane?
Impedancja 32 ohm 250 czy 600 są przeznaczony do różnych urządzeń, parametr sam w sobie trudno określić go jako minimalne. Wtyk Jack 3.5 ma być jeden 4 pinowy czy dwa?

Odpowiedź:
Wtyk Jack 3.5 ma być jeden 4 pinowy. Przeznaczenie laptop z gniazdem Headset.

Jednocześnie Zamawiający informuje, że termin składania ofert **uległ zmianie** i jest wyznaczony na dzień **27 marca 2019 roku do godziny 10.00.** Miejsce składania ofert pozostaje bez zmian.

Przewodniczący Komisji Przetargowej