Mszanowo 19.03.2019 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.**

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 jakie wpłynęły do Zamawiającego, wyjaśniam:

**Pytanie nr 1**

„Wymagania techniczne dla routera zostały określone z ewidentnym naruszeniem zasad konkurencyjności postępowania przetargowego oraz standardów określających dopuszczony sposób opisywania przedmiotu zamówienia. Specyfikacja w przetargu jest dosłownie przepisaniem 1:1, praktycznie nawet w tej samej kolejności, szeregu parametrów technicznych charakterystycznych wyłącznie dla urządzenia firewall/Route Fortigate FG-30E firmy Fortinet. W załączeniu zrzut ekranu strony dokumentacji przedstawiającej zestawienie parametrów. Jak porówna się je z zestawieniem z Państwa SIWZu od razu rzuca się w oczy przepisanie parametrów z dokumentacji producenta do Państwa OPZ-tu. https://www.fortinet.com/content/dam/fortinet/assets/data-heets/FortiGate\_FortiWiFi\_30E.pdf

Zamawiający używa nawet nazw własnych producenta: np. Maksymalna liczba FortiToken 20, Maksymalna liczba zarejestrowanych FortiClient-o?w 200. Wnioskujemy o taką zmianę wymagań techniczno-funkcjonalnych, aby, zgodnie w wytycznymi UPzp pasowany urządzenia min. trzech różnych producentów.”

***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:***

System bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w warstwie aplikacji, Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1.W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2.Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.3.Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1.System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45., 2.System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3.W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 100 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

4.System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1.W zakresie Firewall’a obsługa nie mniej niż 900 tys. jednoczesnych połączeń oraz 15.000 nowych połączeń na sekundę. 2.Przepustowość Stateful Firewall: nie mniej niż 0.95 Gbps.

3.Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 400 Mbps.

4.Wydajność szyfrowania IPSec VPN: nie mniej niż 75 Mbps.

5.Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 300 Mbps.

6.Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 150 Mbps. 7.Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 125 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1.Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2.Kontrola Aplikacji. 3.Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5.Ochrona przed atakami - Intrusion Prevention System. 6.Kontrola stron WWW.

7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8.Zarządzanie pasmem (QoS, Traffic shaping). 9.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10.Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11.Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

1.Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2.System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.

- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3.W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1.System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: - Wsparcie dla IKE v1 oraz v2. - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). - Obsługa protokołu Diffie-Hellman grup 19 i 20. - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2.System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1.W zakresie routingu rozwiązanie powinno zapewniać obsługę: - Routingu statycznego.

- Policy Based Routingu. - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1.System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2.Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3.System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1.Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2.System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3.System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4.System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

Ochrona przed atakami

1.Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2.System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3.Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4.Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5.System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6.Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7.Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola alikacji

1.Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2.Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3.Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4.Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5.Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1.Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2.W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3.Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4.Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5.Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1.System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- 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.

2.Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3.Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie: 1.Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2.Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3.Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4.System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5.System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6.Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1.Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2.W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3.Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4.Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: - ICSA lub EAL4 dla funkcji Firewall. - ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW. - ICSA dla funkcji SSL VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen. W ramach serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

**Pytanie nr 2**

Zamawiający ograniczył wybór oprogramowania AV (wymóg otrzymania w teście AV TEST dla klientów biznesowych dla Windows 10 na grudzień 2018 ocen w kategorii Ochrona – 6; Wydajność – 6; Użyteczność - 6 ) do 3 producentów tj. Symantec, Kaspersky i Trend Micro.

Z informacji jakie uzyskaliśmy od dystrybutora oprogramowania AV wynika że żaden z tych 3 producentów oprogramowania antywirusowego nie oferuje licencji o długości ochrony 5 lat.

Maksymalny okres długości licencji to 3 lata

***Odpowiedź:***

W załączniku nr 6 do SIWZ – opisie przedmiotu zamówienia poz. 4 „Oprogramowanie antywirusowe wersja EDU”, Zamawiający zmienia zapisy w ten sposób, że:

- w punkcie 4 w kolumnie drugiej (Oprogramowanie antywirusowe wersja EDU (licencja 5 lat)), wykreśla zapis (licencja 5 lat),

- w punkcie 4 w kolumnie trzeciej (specyfikacja techniczna) tekst „Licencja na stacje robocze i urządzenia mobilne w szkole na okres 5 lat” zastępuje zapisem „Licencja na stacje robocze i urządzenia mobilne w szkole min 12 miesięcy.”

Jednocześnie Zamawiający informuje, że termin składania ofert **nie ulega zmianie**   
i jest wyznaczony na dzień **22 marca 2019 roku do godziny 10.00.** Miejsce składania ofert pozostaje bez zmian.

**Przewodniczący Komisji**

**Przetargowej**