Treść zapytań wraz z odpowiedziami - zmiana treści SIWZ

Prezydent Miasta Lublin informuje, że w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego na **dostawę urządzeń sieciowych do szkół w ramach projektu „Opracowanie i wdrożenie zintegrowanego systemu informatycznego dla jednostek oświatowych miasta Lublin”** wpłynęły zapytania dotyczące następujących kwestii:

1) Rozdział 1.1 sekcja "Zarządzanie"
W tym wymaganiu Zamawiający oczekuje rozwiązania które jednocześnie zapewni możliwość centralnego zarządzania całą infrastrukturą a dodatkowo spełni funkcję centralnego repozytorium logów. Taka architektura ogranicza konkurencyjność a jednocześnie nie gwarantuje najwyższego poziomu bezpieczeństwa wynikającego z rozdzielenia warstwy zarządzającej od warstwy agregującej i analizującej logi. Wnosimy o zmianę charakteru zapisów w sposób umożliwiający realizację wymagania w oparciu o dwa niezależne urządzenia wirtualne uruchomione w środowisku ESX, których zarządzanie odbywa się z jednego, wspólnego interfejsu.

Odpowiedź:
Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy - dokumentacja do projektu - dostawa urządzeń sieciowych do szkół w ramach projektu "Opracowanie i wdrożenie zintegrowanego systemu informatycznego dla jednostek oświatowych miasta Lublin", Urząd Miasta Lublin., rozdział 1.1, punkt „Zarządzanie”, zdanie czwarte w następujący sposób:

JEST:
System zarządzania musi zostać dostarczony w formie wirtualnego urządzenia uruchomionego w środowisku VMware ESX, gdzie warstwa wirtualizacyjna zadba o wysoką dostępność systemu zarządzania.

OTRZYMUJE BRZMIENIE:
System zarządzania musi zostać dostarczony w formie zwirtualizowanej pod środowisko VMware ESX. Może składać się on maksymalnie z dwóch niezależnych urządzeń wirtualnych. Interfejs zarządzania musi być wspólny dla całego dostarczonego środowiska.

2) Rozdział 3.1 sekcja "Parametry wymagane", punkt 5 oraz Rozdział 3.1 punkt 5
Wymaganie nie znajduje zastosowania w tej formie w kontekście omawianego projektu i oznacza eliminację rozwiązań konkurencyjnych bez uzasadnienia technicznego. Wnosimy o zmianę zapisu do postaci: "System musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchumienie jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż jeden z wymienionych: BGP, RIP lub OSPF".

Odpowiedź:
Zamawiający wyjaśnia, że jest dostawcą usług informatycznych dla różnych jednostek miejskich. W związku z powyższym, zachodzi konieczność obsługi wielu niezależnych tablic routingu oraz protokołów dynamicznego routingu. Zamawiający aktualnie wykorzystuje w posiadanej sieci wiele tablic routingu w postaci odrębnych systemów VRF. Przez to wymaga wsparcia wielu tablic routingu w obrębie pojedynczej instancji systemu zabezpieczeń. Wiele dostępnych na rynku produktów zapewnia takie funkcjonalności. Mając na względzie powyższe Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

3) Rodział 3.1 sekcja "Parametry wymagane", punkt 8
Zamawiający wymaga, aby rozwiązanie zostało dostarczone z konkretnym określonym zestawem interfejsów sieciowych.
Wobec tego iż:
• Zamawiający nie przedstawił schematu planowanego połączenia do obecnej infrastruktury sieciowej uzasadniającego taki zestaw portów
• Wymagane wydajności nie uzasadniają stosowania interfejsów 40Gbps (urządzenie nie zapewnia takiej wydajności, a wydajność większa niż 10Gbps może być zapewniona przez zastosowanie redundancji na interfejsach 10Gbps za pomocą otwartego i wspieranego przez większość urządzeń sieciowych protokołu LACP)
Wnosimy o zmianę wymagania w następujący sposób:
„Urządzenie musi posiadać minimum:
16 portów SFP/SFP+ 1/10Gbps lub 8 portów SFP 1Gbps i 8 portów SFP+ 10 Gbps
4 porty 1000Base-TX lub 4 Porty RJ45 1Gbps
1 port do zarządzania urządzeniem typu out-of-band 1GE RJ45
1 port konsoli RJ45
1 port USB"

Odpowiedź:
Zamawiający zawarł w SIWZ wszystkie niezbędne parametry techniczne dla zamawianych urządzeń umożliwiające przygotowanie oferty. Wobec powyższego dodatkowe informacje w postaci schematu nie są niezbędne do prawidłowego przygotowania oferty. Zamawiający wyjaśnia, że urządzenia na styku między operatorem i siecią zamawiającego będą pracować w warstwie L3, co w znaczny sposób ogranicza funkcjonalność LACP.
Standardem w nowo zbudowanej w 2018 roku sieci szkieletowej Zamawiającego są połączenia 40Gb QSFP+. W związku z powyższym, wydajności i dobór interfejsów są ściśle związane z posiadaną przez Zamawiającego infrastrukturą i tym samym są jak najbardziej uzasadnione. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

4) Rodział 3.1 sekcja "Parametry wymagane", punkty 13 oraz 14
Zamawiający wymaga, aby rozwiązanie posiadało wydajność 18 Gbps dla ruchu z włączoną kontrolą aplikacji oraz 9 Gbps dla ruchu z włączoną dodatkowo inspekcją AV, anty-spyware, IPS i URL Filtering.
W związku z tym, iż:
• Zamawiający nie podał uzasadnienia dla konkretnych wartości,

• Zamawiający nie wyspecyfikował typu ruchu jaki ma być analizowany
• Producenci podają różne wartości dla różnej charakterystyki ruchu
• Tylko niektórzy producenci mają osobny wydzielony profil „antyspyware", zazwyczaj
funkcjonalność anty-spyware jest zapewniona w ramach funkcjonalności Antywirus.
• Większość producentów jak i niezależnych firm testujących rozwiązania Enterprise
Firewall/NextGeneration Firewall podaje specyfikację ruchu ThreatProtection jako kontrola aplikacji, IPS i antywirus (bez kategoryzacji URL).
Wnosimy o zmianę wymagania w następujący sposób:
„System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 18 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola antymalware(antywirus), IPS, rozpoznawanie aplikacji) i obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń. Zamawiający dopuszcza rozwiązanie, w którym dla ruchu HTTP 64K i włączonej kontroli aplikacji osiągnie ono wydajność 16Gbps i dla ruchu Enterprise IMIX z kontrolą zawartości tj. Antywirus, IPS, kontrola aplikacji zostanie osiągnięta wydajność 5 Gbps"

Odpowiedź:
Zamawiający wyjaśnia, że dopuszcza aby do realizacji ochrony przed Spyware był wykorzystywany moduł Antywirus lub Antymalware jeżeli funkcjonalnie spełnia wymagania SIWZ. W kwestii profilu antyspyware Zamawiający ma na celu uzyskanie określonej funkcjonalności bez względu na to, jaki moduł jest do tego wykorzystywany.
W świetle powyższego Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.1 punkt 14 w następujący sposób:

JEST:
14. System musi posiadać przepływność w ruchu full-duplex nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering).

OTRZYMUJE BRZMIENIE:
14. System musi posiadać przepływność w ruchu full-duplex nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola aplikacji, anty-wirus, anty-spyware, IPS).

5) Rodział 3.1 sekcja "Parametry wymagane", punkt 19 oraz Rozdział 3.2 punkt 17
Zamawiający wymaga, aby implementacja i realizacja funkcjonalności polityki bezpieczeństwa rozwiązania Firewall była zapewniona w określony i konkretny sposób specyficzny tylko dla wybranych producentów.
Ponieważ różne rozwiązania zapewniają tą samą funkcjonalność w różny sposób (np. alarmowanie czy i rejestrowanie zdarzeń/reakcje zabezpieczeń czy rejestrowanie zdarzeń mogą być zaimplementowane i definiowane w osobnych politykach) wnosimy o zmianę wymagania w następujący sposób umożliwiając dopuszczenie szerszej gamy rozwiązań:
„Rozwiązanie musi umożliwiać budowę polityki zabezpieczeń firewall, która musi

uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie. Rozwiązanie ma posiadać możliwość zarządzania pasmem w sieci w oparciu o: priorytet, pasmo gwarantowane, pasmo maksymanle, oznaczenia DiffServ".
Zamawiający dopuszcza, aby realizacja poszczególnych wymagań polityki była konfigurowana i realizowana przez odpowiednie moduły funkcjonalne".

Odpowiedź:
Zamawiający wyjaśnia, że wymaga spełnienia określonych funkcjonalności a nie sposobu ich realizacji. Z uwagi na elastyczność konfiguracji polityk bezpieczeństwa oraz eliminację błędów w konfiguracji, które mogą powstać przy zbyt złożonych sposobach budowania polityk bezpieczeństwa, Zamawiający podtrzymuje wymagania w tym zakresie. Na rynku istnieje wiele produktów spełniających to wymaganie.

6) Rodział 3.1 sekcja "Parametry wymagane", punkt 21 oraz Rozdział 3.2 punkt 19
Zamawiający określa sposób realizacji wymagania, którego realizacja może odbywać się innymi metodami z równą lub większą skutecznością przy wykorzystaniu rozwiązań konkurencyjnych.
Ponieważ różne rozwiązania zapewniają tą samą funkcjonalność w różny sposób (a skuteczność wielu z nich jest potwierdzona w niezależnych testach renomowanych organizacji i firm trzecich) wnosimy o zmianę wymagania w następujący sposób umożliwiając dopuszczenie równoważnych rozwiązań innych producentów:
"System musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowanie i szyfrowania (włączanie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i/lub analizę heurystyczną."

Odpowiedź:
Zamawiający wyjaśnia, że z uwagi na krytyczne znaczenie budowanej infrastruktury dla bezpieczeństwa placówek oświatowych, w szczególności odpowiedniej identyfikacji aplikacji dostarczających niepożądane dla uczniów treści, Zamawiający musi mieć możliwość elastycznego tworzenia reguł bezpieczeństwa tak, aby zapewnić maksymalny poziom bezpieczeństwa użytkowników. Zamawiający uważa, że równocześnie zastosowanie identyfikacji przez co najmniej dwa mechanizmy jest skuteczniejsze niż zastosowanie tylko jednego mechanizmu. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

7) Rodział 3.1 sekcja "Parametry wymagane", punkt 22 oraz Rozdział 3.2 punkt 20
Zamawiający wymaga aby rozwiązanie realizowało swoje zadania z wydajnością która jest
charakterystyczna dla wybranych kilku produktów dostępnych na rynku. Oczekiwanie wydajności firewall i kontroli aplikacji na tym samym poziomie nie znajduje żadnego uzasadnienia technicznego lub projektowego, dlatego też wnosimy o zmianę zapisu do postaci:
"Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć,

że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. Wydajność kontroli firewall może być większa bądź równa wydajności kontroli aplikacji, która to kontrola aplikacji ma odbywać się w ruchu fullduplex z wydajnością nie mniejszą niż wskazano w wymaganiach wydajnościowych"

Odpowiedź:
Zamawiający wyjaśnia, że współczesna ochrona zasobów sieciowych musi opierać się o rozpoznawanie aplikacji. Obecnie ochrona wyłącznie na poziomie sieciowym jest niewystarczająca.
Tym samym Zamawiający definiując wymagania dla firewalla aplikacyjnego określa oczekiwany poziom wydajności urządzenia (wymaga aby wydajność dla firewalla aplikacyjnego i firewalla L3/L4 była na tym samym poziomie). W świetle powyższego Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

8) Rodział 3.1 sekcja "Parametry wymagane", punkt 23 oraz Rozdział 3.2 punkt 21 zmianę do Opisany przez Zamawiającego sposób realizacji wymagania nie posiada uzasadnienia technicznego jako, że mechanizm tworzenia polityki poprzez dodatkowe profile w żaden sposób nie zmniejsza skuteczności rozwiązania w zakresie rozpoznawania i kontroli aplikacji. Dlatego wnioskujemy o usunięcie tego zapisu lub jego zmianę do następującej postaci:
"Zezwolenie dostępu do aplikacji może odbywać się w regułach polityki firewall lub może być definiowane przez dodatkowe profile".

Odpowiedź:
Zamawiający wyjaśnia, że zamawiana infrastruktura będzie tworzyć krytyczną usługę dotyczącą bezpieczeństwa jednostek oświatowych. Intencją zamawiającego jest osiągnięcie odpowiedniej funkcjonalności w możliwie prosty i czytelny sposób. Złożona, wielopoziomowa konfiguracja stwarza ryzyko popełnienia błędów ludzkich. Dlatego Zamawiający dąży do implementacji rozwiązania oferującego maksymalnie odporny na błędy system. Ponadto, zaproponowany w pytaniu sposób budowania tych polityk, ogranicza możliwości Zamawiającego w zakresie kreowania polityk bezpiecznego dostępu do aplikacji. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

9) Rodział 3.1 sekcja "Parametry wymagane", punkt 26 oraz Rozdział 3.2 punkt 24 Wymagana przez Zamawiającego lista plików jednoznacznie wskazuje na rozwiązanie tylko jednego producenta. Poszczególni producenci realizują blokowanie plików w oparciu własną (niejednokrotnie równie rozbudowaną choć nie identyczną) listę formatów. Z tego powodu wnosimy o dopuszczenie dodatkowo następującego zapisu równoważnego:
"Zamawiający dopuszcza rozwiązanie w którym system musi pozwalać na blokowanie transmisji plików, nie mniej niż: .7z, arj, cab, lzh, rar, tar, zip, bzip, gzip, bzip2, xz, bat, msc, uue, mime, base64, binhex, elf, exe, hta, html, jad, class, cod, javascript, msoffice, msofficex, fsg, upx, petite, aspack, prc, sis, hlp, activemime, jpeg, gif, tiff, png, bmp, ignored, unknown, mpeg, mov, mp3, wma, wav, pdf, avi, rm, torrent, hibun, msi. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia."

Odpowiedź:
Zamawiający wyjaśnia, że wymaga opcji blokowania plików bezpośrednio związanych z charakterem pracy zamawiającego jak i związanych ze środowiskiem pracy zamawiającego.
Jednocześnie Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.1, punkt 26 i rozdział 3.2, punkt 24 w następujący sposób:

JEST:
System musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

OTRZYMUJE BRZMIENIE:
System musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, doc, docx, ppt, pptx, xls, xlsx, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

10) Rozdział 3.1 sekcja "Parametry wymagane", punkt 28 oraz Rozdział 3.2 punkt 26
Zamawiający wymaga, aby rozwiązanie firewall zapewniało ochronę przed atakami „Drive-by-Download" w sposób wspierany tylko przez jednego producenta i dodatkowo nie gwarantujący tej ochrony i pozostawiający użytkownikowi decyzyjność w sprawie blokowania danego pliku.
W związku z tym iż powyższa ochrona nie gwarantuje skutecznej ochrony przed atakiem tego typu oraz jest ona opisem funkcjonalności wskazującym na konkretne rozwiązanie, wnosimy o zmianę jego usunięcie lub zmianę na następujące, aby dopuści rozwiązania równoważne i konkurencyjne do opisanego:
„System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download".

Odpowiedź:
Zamawiający wyjaśnia, że wymaga, aby oferowane rozwiązanie zapewniało skuteczną ochronę przed atakami typu „Drive-by-download".
W związku z powyższym Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.1, punkt 28 i rozdział 3.2, punkt 26 w następujący sposób:

JEST:
System musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.

OTRZYMUJE BRZMIENIE:
System musi zapewniać ochronę przed atakami typu „Drive-by-download".

11) Rozdział 3.1 sekcja "Parametry wymagane", punkt 39 oraz Rozdział 3.2 punkt 37
Wymaganie postawione w postaci sugerowanej przez Zamawiającego ogranicza wachlarz dostępnych sposobów realizacji oczekiwanej funkcjonalności. Dlatego też wnosimy dopuszczenie zapisu w postaci:
"System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na postawie znaczników DSCP lub też per adres IP czy też per aplikacja. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego".

Odpowiedź:
Zamawiający wyjaśnia, że w sieci Zamawiającego stosowane są urządzenia znakujące ruch znacznikami DSCP w celu zarządzania pasmem. Dlatego też wymaganiem Zamawiającego jest, aby oferowane urządzenie wspierało ww. funkcjonalność. Tym samym Zamawiający podtrzymuje wymagania SIWZ.

12) Rozdział 3.1 sekcja "Parametry wymagane", punkt 50 oraz Rodział 3.2 punkt 48
W związku iż XML nie jest standardem API, wnosimy o dopuszczenie rozwiązań wykorzystujących inne standardy niż XML i tym samym zmianę zapisu na następującą treść:
„System zabezpieczeń firewall musi być wyposażony w interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).”

Odpowiedź:
Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.1, punkt 50 i rozdział 3.2, punkt 48 w następujący sposób:

JEST:
System musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

OTRZYMUJE BRZMIENIE:
System musi być wyposażony w interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

13) Rozdział 3.1 sekcja "Parametry wymagane", punkt 52 oraz Rozdział 3.2 punkt 50
Ze względu na różne sposoby realizacji uwierzytelniania administratorów przez różnych
producentów, wnosimy o zmianę zapisu do postaci:
"System bezpieczeństwa musi umożliwiać uwierzytelniania administratorów za pomocą nie mniej niż 4 następujących metod: bazy lokalnej, serwera LDAP, RADIUS, TACACS+, kerberos, uwierzytelniania dwuskładnikowego

z wykorzystaniem tokenów."

Odpowiedź:
Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.1, punkt 52 i rozdział 3.2, punkt 50 w następujący sposób:

JEST:
System musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.

OTRZYMUJE BRZMIENIE:
System bezpieczeństwa musi umożliwiać uwierzytelniania administratorów za pomocą nie mniej niż: serwera LDAP, Kerberos, uwierzytelniania dwuskładnikowego z wykorzystaniem tokenów, bazy lokalnej i jednej z 2 następujących metod: RADIUS lub TACACS+.

14) Rozdział 3.1 sekcja "Parametry wymagane", punkty 47, 48, 49, 54, 55 oraz Rozdział 3.2 punkt 37 45, 46, 47, 52, 53
Ponieważ ww. wymagania łącznie znacznie ograniczają zbiór produktów je spełniających wnosimy o umożliwienie dostarczenia rozwiązań konkurencyjnych i równoważnych na zasadzie dostarczenia rozwiązania, a nie urządzenia, w związku z tym wnosimy o dodanie następującej preambuły do wymagań specyfikacji rozwiązania".
„Dostarczony 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".

Odpowiedź:
Zamawiający wyjaśnia, że posiada ograniczone zasoby przestrzeni przeznaczonej na instalacje urządzeń, dodatkowo pełna funkcjonalność bezpieczeństwa urządzeń sieciowych zainstalowanych w jednostkach musi być realizowana także w przypadku przerw
w transmisji pomiędzy siecią Zamawiającego a jednostką.
Zarządzanie urządzeniami odbywać się będzie zarówno przez administratorów lokalnych w placówkach oraz przez administratorów Zamawiającego. W związku z powyższym oferowane rozwiązanie musi wspierać szereg różnych scenariuszy dotyczących procesów zarządzania zmianami oraz działania w sytuacjach awaryjnych. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

15) Rozdział 3.1 sekcja "Parametry wymagane", punkt 56 oraz Rozdział 3.2 punkt 54
Weryfikacja wpływu zmian konfiguracji na istniejące polityki bezpieczeństwa

odbywa się w różny sposób u różnych producentów. Dlatego też wnosimy o zmianę zapisu do postaci:
"System musi umożliwiać sprawdzenie wpływu nowo stworzonych polityk bezpieczeństwa na te już istniejące."

Odpowiedź:
Zamawiający wyjaśnia, że wymaga nie tylko sprawdzenia wpływu nowo wprowadzanych polityk na istniejące, ale także sprawdzenia wpływu nowych, pobranych od producenta sygnatur (aplikacji, IPS) na skonfigurowane polityki. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

16) Rozdział 3.1 sekcja "Parametry wymagane", punkt 57 oraz Rozdział 3.2 punkt 55
W związku z tym, że wymaganie jest typowe tylko dla niektórych rozwiązania wnosimy o usunięcie wymagania lub dopuszczenie rozwiązania, gdzie można skonfigurować kilka serwerów syslog jednocześnie bez konieczności robienia tego per polityka.

Odpowiedź:
Zamawiający wyjaśnia, że jest dostawcą usług dla różnych podmiotów, które mają różne wymagania bezpieczeństwa, w szczególności w zakresie logowania zdarzeń/incydentów bezpieczeństwa. Oferowane rozwiązanie nie może zatem ograniczać Zamawiającego w zakresie elastycznego kształtowania konfiguracji logowania w odniesieniu do polityk bezpieczeństwa oraz wymagań usługobiorców. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

17) Rozdział 3.1 sekcja "Parametry wymagane", punkt 64 oraz Rozdział 3.2 punkt 62
Jako, że w zależności od producenta poszczególne funkcjonalności licencjonowane są w różnych sposób, wnosimy z modyfikację zapisu do postaci:
"Zamawiający wymaga możliwości rozbudowy o następujące funkcjonalności wraz z niezbędnymi subskrypcjami/licencjami tam gdzie są one konieczne, jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego"
Reszta zapisów bez zmian.

Odpowiedź:
Zamawiający wyjaśnia, że wymaga możliwości rozbudowy w przyszłości o kolejne funkcje. Mogą być one dostarczone w dowolnie nazwanych/zdefiniowanych kombinacjach licencji/subskrypcji.
W związku z powyższym Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.1, punkt 64 i rozdział 3.2, punkt 62 w następujący sposób:

JEST:
Zamawiający wymaga możliwości rozbudowy o następujące subskrybcje/licencje jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego (...).

OTRZYMUJE BRZMIENIE:

Zamawiający wymaga możliwości rozbudowy o następujące funkcjonalności wraz z niezbędnymi subskrypcjami/licencjami tam gdzie są one konieczne, jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego (...).

18) Rozdział 3.2 punkt 8
Zamawiający wymaga, aby rozwiązanie zostało dostarczone z konkretnym określonym zestawem interfejsów sieciowych.
Wobec tego iż:
• Zamawiający nie przedstawił schematu planowanego połączenia do obecnej infrastruktury
sieciowej uzasadniającego taki zestaw portów
- Realizację podłączenia światłowodu w jednostce oświatowej można uzyskać z wykorzystaniem konwertera odpowiedniego rodzaju, co spowoduje
Wnosimy o zmianę wymagania w następujący sposób:
„Urządzenie musi posiadać minimum:
14x port RJ45 1Gbps".

Odpowiedź:
Zamawiający wyjaśnia, że zdefiniował wydajności i dobór interfejsów w sposób rzetelny i odzwierciedlający obecne i przyszłe potrzeby. Jednocześnie Zamawiający zaznacza, iż wymaganie 12 interfejsów 1Gbps (w tym części z nich jako interfejsów światłowodowych) jest realizowane przez większość liczących się dostawców systemów firewall. Zamawiający będzie wykorzystywał w projekcie moduły SFP zarówno do podłączenia do operatora zewnętrznego jak i integracji z infrastrukturą wewnętrzną jednostek.
Zamawiający nie dopuszcza stosowania zewnętrznych konwerterów światłowodowych w celu uniknięcia tworzenia dodatkowego punktu awarii. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

19) Rozdział 3.2 punkt 11
Zamawiający wymaga wsparcia (jednocześnie) 4094 znaczników VLAN.
Ponieważ nie ma to uzasadnienia technicznego w jednostkach oświatowych, wnosimy o zmianę ilości jednocześnie stworzonych interfejsów VLAN na 256 – liczba ta jest na tyle duża, że nie zostanie przekroczona podczas nawet bardzo niestandardowej konfiguracji sieci.
W związku z tym wnosimy o zmianę wymagania na:
„System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 256 jednoczesnych znaczników VLAN."

Odpowiedź:
Zamawiający wyjaśnia, że na rynku dostępnych jest wiele różnych produktów, które wspierają podaną liczbę. Zamawiający oczekuje w tym zakresie elastyczności i swobody działania oraz rozwoju. W związku z powyższym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

20) Rozdział 3.2 punkt 12 oraz 13

Zamawiający wymaga, aby rozwiązanie posiadało wydajność 900 Mbps dla ruchu z włączoną kontrolą aplikacji oraz 600 Mbps dla ruchu z włączoną dodatkowo inspekcją AV, anty-spyware, IPS i URL Filtering.
W związku z tym, iż:
- Zamawiający nie podał uzasadnienia dla konkretnych wartości,
- Zamawiający nie wyspecyfikował typu ruchu jaki ma być analizowany
- Producenci podają różne wartości dla różnej charakterystyki ruchu
- Tylko niektórzy producenci mają osobny wydzielony profil „antyspyware", zazwyczaj
funkcjonalność anty-spyware jest zapewniona w ramach funkcjonalności Antywirus.
- Większość producentów jak i form testujących rozwiązania Enterprise Firewall/NextGeneration Firewall podaje specyfikację ruchu ThreatProtection jako kontrola aplikacji, IPS i antywirus (bez kategoryzacji URL)
Wnosimy o zmianę wymagania w następujący sposób:
„System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż
900Mbps dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 600 Mbps dla kontroli zawartości (w tym kontrola antymalware(antywirus), IPS, rozpoznawanie aplikacji) i obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń.
Zamawiający dopuszcza rozwiązanie, w którym dla ruchu HTTP 64K i włączonej kontroli aplikacji osiągnie wydajność 900 Mbps i dla ruchu Enterprise IMIX z kontrolą zawartości tj. Antywirus, IPS, kontrola aplikacji zostanie osiągnięta wydajność 240 Mbps"

Odpowiedź:
Zamawiający wyjaśnia, że wskazał wszelkie potrzebne dane dla doboru urządzeń niezbędnych dla realizacji zadań i celów które chce osiągnąć, w tym podane zostały podstawowe parametry wydajnościowe.
W kwestii profilu antyspyware Zamawiający ma na celu uzyskanie określonej funkcjonalności bez względu na to, jaki moduł jest do tego wykorzystywany - Zamawiający dopuszcza tym samym by do realizacji ochrony przed Spyware był wykorzystywany moduł Antywirus lub Antymalware jeżeli funkcjonalnie jest w stanie ochronić zasoby Zamawiającego przed oprogramowaniem Spyware.
Zamawiający akceptuje zmianę wymagań w zakresie, iż wydajność ruchu Threat Prevention jest traktowana jako kontrola aplikacji, antywirus i IPS. (bez URL Filtering).
W związku z powyższym Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3.2, punkt 13 w następujący sposób:
JEST:
System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 600 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering).

OTRZYMUJE BRZMIENIE:
System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej

niż 600 Mbit/s dla kontroli zawartości (w tym kontrola kontrola aplikacji, anty-wirus, anty-spyware, IPS).

21) Rodział 3.2 punkt 52
Zamawiający wymaga zastosowanie dysku twardego o pojemności 240GB, co nie znajduje uzasadnienia projektowego, a dodatkowo jest spełniane tylko przez wybrane urządzenia np. CheckPoint i PaloAlto. Dlatego też wnosimy o zmianę wymogu do postaci:
"System zabezpieczeń firewall musi posiadać wbudowany dysk twardy do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB."

Odpowiedź
Zamawiający wyjaśnia, że wymaga stosowania dysku o pojemności nie mniejszej niż 240 GB, w celu lokalnego zapewnienia funkcji monitorowania, analizy logów i raportowania. W związku z dużym ryzykiem występowania różnych incydentów bezpieczeństwa na styku sieci jednostki oświatowej z siecią miejską Zamawiający wymaga zastosowania nośników
o możliwie dużej pojemności, mając na uwadze okres trwałości projektu oraz okres dalszej eksploatacji wdrażanego rozwiązania. Na rynku występuje katalog produktów spełniających powyższe wymagania. Tym samym Zamawiający podtrzymuje wymagania SIWZ w tym zakresie.

22) Rozdział 3.3 całość oraz punkt 27
Wnosimy o zmianę zapisu dotyczącego wymagania związanego z systemem zarządzania, tak aby system zarządzania i logowania mogły być osobnymi platformami sprzętowymi lub wirtualnymi pochodzącymi jednego, tego samego co firewall, producenta.
„Dostarczony 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, w tym system zarządzania i logowania 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.

Odpowiedź:
Zamawiający dokonuje zgodnie z art. 38 ust. 4 ustawy z dnia 29.01.2004r. Prawo zamówień publicznych (tj. Dz.U. z 2017r. poz. 1579 ze zm.) zmiany treści Specyfikacji Istotnych Warunków Zamówienia, załącznika nr 1 do SIWZ i nr 1 do umowy, rozdział 3. poprzez usunięcie punktu 27 oraz renumerację pkt 28-29. Usunięta treść: „27. System zarządzania, logowania i raportowania musi być dostarczony jako dedykowane urządzenie/urządzenia sieciowe."

Jednocześnie w związku z dokonaną zmianą treści SIWZ, Zamawiający działając na podstawie art. 38 ust. 4 ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004r. (t.j. Dz. U. z 2017 r. poz. 1579 ze zm.) dokonuje zmiany pkt 11 Specyfikacji Istotnych Warunków Zamówienia, który otrzymuje następujące brzmienie:

"11.1 Oferty należy składać w Biurze Zamówień Publicznych Urzędu Miasta Lublin, Plac Litewski 1, pokój nr 8.
11.2 W postępowaniu wezmą udział tylko te oferty, które wpłyną do Zamawiającego do dnia 06.09.2018 r. do godz. 11:30 na adres wskazany w pkt 11.1. Decydujące znaczenie dla oceny zachowania powyższego terminu ma data i godzina wpływu oferty na adres wskazany w pkt 11.1., a nie data jej wysłania przesyłką pocztową czy kurierską.
11.3 Otwarcie ofert nastąpi w Biurze Zamówień Publicznych Urzędu Miasta Lublin, Plac Litewski 1, pokój 302 dnia 06.09.2018 r. o godzinie 12:00."

Pozostałe zapisy specyfikacji istotnych warunków zamówienia pozostają bez zmian.

Z up. PREZYDENTA MIASTA LUBLIN
Elżbieta Daszyńska
DYREKTOR
Biura Zamówień Publicznych

W załączeniu:
1. Aktualnie obowiązujący załącznik nr 1 do SIWZ i nr 1 do umowy - dokumentacja do projektu - dostawa urządzeń sieciowych do szkół w ramach projektu "Opracowanie i wdrożenie zintegrowanego systemu informatycznego dla jednostek oświatowych miasta Lublin", Urząd Miasta Lublin.