WARSZAWSKI UNIWERSYTET MEDYCZNY
MEDICAL UNIVERSITY OF WARSAW

Dział Zamówień Publicznych

Wasze pismo z dnia	Znak	Nasz znak	Data
		AEZ/362/1334/2017/EJ	11.08.2017 r.

Wykonawcy
biorący udział w postępowaniu
AEZ/S-121/2017

Wyjaśnienia oraz zmiana treści SIWZ

Działając na podstawie art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), Warszawski Uniwersytet Medyczny, ul. Żwirki i Wigury 61, 02-091 Warszawa, Zamawiający w postępowaniu p.n. ***Dostawa sprzętu komputerowego i systemów bezpieczeństwa w podziale na pakiety; znak sprawy AEZ/S-121/2017***, informuje, że wpłynęły do Zamawiającego pytania o treści:

Pytanie 1:
Dotyczy wymagania nr 5 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, "20 portów 1G/10G SFP/SFP+" zamiast "4 porty Ethernet 100M/1G/10G, 16 portów 1G/10G SFP/SFP+"? Jakie wkładki miedziane/optyczne powinny zostać wycenione?

Odpowiedź:
Zamawiający doprecyzował wymagania dot. ilości portów oraz wkładek. Powyższe informacje zawarte są w poz. 5 Załącznika nr 2.1:
„System zabezpieczeń firewall musi być wyposażony w co najmniej:

- *4 porty Ethernet 100M/1G/10G i 16 portów 1G/10G SFP/SFP+ lub 20 portów 1G/10G SFP/SFP+. W obu przypadkach należy dostarczyć 2 wkładki SFP+ optyczne 10G LC oraz wyposażyć pozostałe wolne porty we wkładki miedziane SFP 1G w każdym urządzeniu klastra.*
- *4 porty 40G QSFP+."*

Pytanie 2:
Dotyczy wymagania nr 7 z załącznika nr 2.1
Taki sposób sprecyzowania wymagania znamionuje preferencję dla konkretnego producenta. Czy Zamawiający zaakceptuje rozwiązanie równoważne pod względem trybów pracy konfigurowalnych w inny sposób? Np. konfiguracja L2 per cały wirtualny system, konfiguracja L1 per para interfejsów w ramach systemu wirtualnego L3?

Odpowiedź:
Zamawiający dokonał zmiany wymagań z poz. 7 oraz ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.
Powyższe informacje zawiera obecnie poz. 110 Załącznika nr 2.1 do SIWZ:
„Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę w trybach rutera, przełącznika, pasywnego nasłuchu i transparentnym jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.)."

Pytanie 3:
Dotyczy wymagania nr 9 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Czy Zamawiający zaakceptuje rozwiązanie posiadające oddzielną tablicę routingu per system wirtualny? Czy ma być dostarczona licencja na 20 systemów wirtualnych?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 8 Załącznika nr 2.1 do SIWZ.

Pytanie 4:
Dotyczy wymagania nr 20 z załącznika nr 2.1
Wymaganie 20 stoi w sprzeczności z wymaganiem 36. Prosimy o określenie, czy kategoria URL ma być elementem klasyfikującym czy elementem filtrującym po zakończeniu etapu klasyfikacji.

Odpowiedź:
Zamawiający informuje, że są to dwie różne funkcjonalności.
Zamawiający pozostawia zapisy SIWZ zakresie poz. 20 bez zmian. Powyższy zapis stanowi obecnie poz. 18 i Załącznika nr 2.1 do SIWZ.
Zamawiający ustanowił spełnienie wymagań z poz. 36 warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert. Powyższe informacje zawiera obecnie poz. 100 Załącznika nr 2.1 do SIWZ.

Pytanie 5:
Dotyczy wymagania nr 21 z załącznika nr 2.1
Tak postawione wymaganie preferuje konkretnego producenta. Czy Zamawiający uzna rozwiązanie za równoważne, jeżeli zapewni blokowanie wszystkich wykonywalnych plików w mailach, blokowanie znacznie dłuższej listy plików na postawie nagłówka MIME (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) oraz dodatkowo umożliwia wykorzystanie tworzenia sygnatur IPS do plików nie będących na wymaganej liście?

Odpowiedź:
Zamawiający rozdzielił ww. pozycję na dwie: poz. 19 – wymaganie obligatoryjne do spełnienia:
„System zabezpieczeń firewall 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, pdf, pgp, pif, pl, reg, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia"
oraz poz. 96 – funkcjonalność fakultatywną, niekonieczną do zaoferowania:
„System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików mdi, ocx, sh"

Pytanie 6:
Dotyczy wymagania nr 23 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Czy Zamawiający zaakceptuje rozwiązanie umożliwiające opcję „kontynuuj" w przypadku transmisji stron, które są blokowane zgodnie z polityką bazującą na sygnaturach oraz danych z Sandbox?

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.
Powyższe informacje zawiera obecnie poz. 98 Załącznika nr 2.1 do SIWZ.

Pytanie 7:
Dotyczy wymagania nr 28 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Czy Zamawiający zaakceptuje rozwiązanie wykonujące inspekcję ruchu SSH pod kątem funkcji Exec, Port-Forward, SSH-Shell, X11-Filter?

Odpowiedź:

Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 24 Załącznika nr 2.1 do SIWZ.

Pytanie 8:
Dotyczy wymagania nr 31 z załącznika nr 2.1
Mechanizmy Single Sign On mogą być realizowane przez różne protokoły, np. RADIUS, który jest bardziej skalowalny i nie jest konieczne zbieranie wielu wiadomości syslog na NGFW. Czy Zamawiający dopuści machanizm SSO bazujący na RADIUS zamiast syslog. Jeżeli SSO/syslog jest wymaganiem krytycznym, czy Zamawiający dopuści rozwiązanie, gdzie zastosowany zostanie dodatkowy serwer w postaci maszyny wirtualnej do konwersji wiadomości syslog na mechanizm SSO producenta, ilu użytkowników ma wspierać ta funkcja?

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.
Powyższe informacje zawiera obecnie poz. 99 Załącznika nr 2.1 do SIWZ.

Pytanie 9:
Dotyczy wymagania nr 32 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta.
Nagłówek X-Forwarded-For może być wykorzystany np. do wzbogacania logów z ataków przeprowadzonych przez użytkowników proxy. Czy taka funkcjonalność spełni to wymaganie?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 27 Załącznika nr 2.1 do SIWZ.

Pytanie 10:
Dotyczy wymagania nr 36 z załącznika nr 2.1
Wymaganie 36 stoi w sprzeczności z wymaganiem 20. Prosimy o określenie, czy kategoria URL ma być elementem klasyfikującym czy elementem filtrującym po zakończeniu etapu klasyfikacji.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 4.

Pytanie 11:
Dotyczy wymagania nr 45 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, gdzie ręczne tworzenie sygnatur anty-spyware dotyczy silnika IPS, a automatyczne sygnatury są dostarczane przez sieć producenta oraz sandbox?

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.
Powyższe informacje zawiera obecnie poz. 102 Załącznika nr 2.1 do SIWZ.

Pytanie 12:
Dotyczy wymagania nr 50 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Czy Zamawiający jest skłonny wykreślić to wymaganie lub doprecyzować o jakie rodzaje poświadczeń chodzi: id, hasło, certyfikat, token oraz o jakie mechanizmy przekazywania poświadczeń?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian.
W celu zapewnienia maksymalnego bezpieczeństwa wymagane jest blokowanie wpisywanego przez użytkownika swojego loginu z wewnętrznego systemu autentykacji/autoryzacji (w domyśle:

również hasła) rozpoznawanego na podstawie jego korelacji z informacją posiadaną przez urządzenie na temat użytkownika, który nawiązał tę sesję.
Powyższy zapis stanowi obecnie poz. 42 Załącznika nr 2.1 do SIWZ.

Pytanie 13:
Dotyczy wymagania nr 52 z załącznika nr 2.1
Czy Zamawiający zaakceptuje rozwiązanie, gdzie wysyłamy wszystkie dozwolone pliki do Sandbox oraz/lub do Sandbox cloud. Czy Sandbox cloud, VM lub HW ma być częścią oferty?

Odpowiedź:
Zamawiający dokonuje zmiany treści poz. 52 (obecnie poz. 44), nadając jej brzmienie:
„Obsługa systemów typu „Sand-Box cloud":

- *System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 9 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.*
- *Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".*
- *Zamawiający wymaga integracji systemu firewall z systemem „Sand-Box cloud" producenta oferowanego urządzenia"*

Jeżeli do spełnienia powyższego warunku wymagana jest dodatkowa licencja, należy ją uwzględnić w ofercie. Powyższy zapis stanowi obecnie poz. 44 Załącznika nr 2.1 do SIWZ.

Pytanie 14:
Dotyczy wymagania nr 58 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta.
Czy Zamawiający jest skłonny do ograniczenia tego wymagania do inspekcji IPS w tunelu GRE?

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.
Powyższe informacje zawiera obecnie poz. 103 Załącznika nr 2.1 do SIWZ.

Pytanie 15:
Dotyczy wymagania nr 59 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Czy Zamawiający jest skłonny do wykreślenia z tego wymagania SAML 2.0 lub dopuszcza dostarczenie oddzielnego serwera uwierzytelniania do integracji z SAML?

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.

Powyższe informacje zawiera obecnie poz. 104 Załącznika nr 2.1 do SIWZ.

Pytanie 16:
Dotyczy wymagania nr 63 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta.
Większość topowych producentów NGFW posiada możliwość integracji z VMWare w środowisku NSX.

Czy Zamawiający posiada środowisko VMWare NSX?
Czy Zamawiający wymaga dostarczenia licencji na NGFW w postaci maszyny wirtualnej, na ile hostów VMWare?
Jeżeli zamawiający nie posiada środowiska NSX, prosimy o wykreślenie tego wymagania.

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.
Powyższe informacje zawiera obecnie poz. 108 Załącznika nr 2.1 do SIWZ
W prowadzonym postepowaniu Zamawiający nie wymaga dostarczenia licencji NGFW w postaci maszyny wirtualnej.

Pytanie 17:
Dotyczy wymagania nr 66 z załącznika nr 2.1
To jest typowe wymaganie dla centralnego systemu zarządzania, szczególnie, jeżeli mamy więcej urządzeń NGFW niż jedno. Czy Zamawiający wymaga dostarczenia centralnego systemu zarządzania?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 54 Załącznika nr 2.1 do SIWZ.

Pytanie 18:
Dotyczy wymagania nr 67 z załącznika nr 2.1
To jest typowe wymaganie dla centralnego systemu zarządzania, szczególnie, jeżeli mamy więcej urządzeń NGFW niż jedno. Czy Zamawiający wymaga dostarczenia centralnego systemu zarządzania?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 55 Załącznika nr 2.1 do SIWZ.

Pytanie 19:
Dotyczy wymagania nr 68 z załącznika nr 2.1
Czy zamawiający dopuści system wyposażony w REST API jako spełniający to wymaganie?

Odpowiedź:
Zamawiający dokonał zmiany powyższego wymagania dopuszczając proponowane przez Wykonawcę rozwiązanie. Powyższy zapis stanowi obecnie poz. 56 Załącznika nr 2.1 do SIWZ:
„System zabezpieczeń firewall musi być wyposażony w interfejs XML API lub REST API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)."

Pytanie 20:
Dotyczy wymagania nr 70 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta.
Czy zamawiający jest skłonny zrezygnować z wykorzystania Kerberos w kontekście tego wymagania?
Mechanizmy uwierzytelniania oparte o Kerberos są na ogół wykorzystywane przy dostępie do aplikacji lub np. explicit proxy.

Odpowiedź:
Zamawiający dokonał zmiany powyższego wymagania. Powyższy zapis stanowi obecnie poz. 58 Załącznika nr 2.1 do SIWZ:
„System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS."

Pytanie 21:
Dotyczy wymagania nr 71 z załącznika nr 2.1
Czy zamawiający dopuści rozwiązanie, gdzie uwierzytelnianie administratora odbywa się przez LDAP lub RADIUS oraz istnieje opcja zachowania lokalnego hasła w przypadku niedostępności zdalnych serwerów LDAP lub RADIUS?

Odpowiedź:
Zamawiający dokonuje zmiany treści poz. 71 (obecnie poz. 59), nadając jej brzmienie:
„System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej dwie metody uwierzytelniania: baza lokalna i LDAP lub RADIUS".

Pytanie 22:
Dotyczy wymagania nr 72 z załącznika nr 2.1
Czy zamawiający dopuści rozwiązanie NGFW o mniejszej wielkości storage, jeżeli zostanie dostarczone z dedykowanym systemem logowania i raportowania?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 60 Załącznika nr 2.1 do SIWZ.

Pytanie 23:
Dotyczy wymagania nr 74 z załącznika nr 2.1
Czy te wymaganie będzie spełnione, jeżeli nowe pakiety sygnatur są opisane na stronie producenta? Wymaganie to wymaga wyłączenia automatycznych aktualizacji sygnatur, co w przypadku ataków typu "zero-day" znacznie zmniejsza bezpieczeństwo sieci.

Odpowiedź:
Zamawiający dokonuje zmiany treści poz. 74 (obecnie poz. 62), nadając jej brzmienie:
„System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. Zamawiający dopuszcza sprawdzenie opisu nowych sygnatur na stronie producenta"

Pytanie 24:
Dotyczy wymagania nr 75 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, gdzie filtry ustawiamy na konkretne serwery logowania per rodzaj logu, a nie per polityka.

Odpowiedź:
Zamawiający ustanowił spełnienie powyższego wymagania warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert.

Powyższe informacje zawiera obecnie poz. 106 Załącznika nr 2.1 do SIWZ.

Pytanie 25:
Dotyczy wymagania nr 77 z załącznika nr 2.1
Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta.
Tego typu wymaganie jest właściwe dla platform logowania i raportowania. Czy Zamawiający dopuści rozwiązanie, gdzie funkcje reakcji na zawartość logów będą realizowane przez system logowania i raportowania za pomocą mechanizmów: alert email, SNMP trap, syslog?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 63 Załącznika nr 2.1 do SIWZ.

Pytanie 26:
Dotyczy wymagania nr 79 z załącznika nr 2.1

Wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta.
Tego typu wymaganie jest właściwe dla platform logowania i raportowania. Czy Zamawiający dopuści rozwiązanie, gdzie funkcje generowania konfigurowalnych będą realizowane przez system logowania i raportowania?
Warto zauważyć, że Zamawiający wymaga klastra NGFW, w takim przypadku dobre praktyki wymagają przechowywania logów i raportów we wspólnym repozytorium odzwierciedlającym stan całej sieci.

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 65 Załącznika nr 2.1 do SIWZ.

Pytanie 27:
Dotyczy wymagania nr 83 z załącznika nr 2.1
Czy ma być zapewniona wysoka dostępność dla systemu zarządzania? Dlaczego wymagana jest licencja dla 25 firewalli. Ile czasu powinny być przechowywane logi dla szybkiej analityki, a ile w formie zarchiwizowanej, jaka jest przewidywana ilość nowych sesji na sekundę, które będą logowane?

Odpowiedź:
Zamawiający nie wymaga wysokiej dostępności (klastra) systemu zarządzania. Docelowo Zamawiający planuje podłączyć dodatkowe urządzenia do systemu zarządzania. Zamawiający nie jest w stanie oszacować ilości nowych sesji na sekundę, które będą logowane oraz czasu przechowywania logów.
Pytanie 28:
Dotyczy warunku opisanego w propozycji umowy, §3 pkt 6
„Wykonawca zapewnia, ze wszelkie instrukcje niezbędne do wykorzystania dostarczonego przedmiotu umowy przez użytkowników Zamawiającego, dostarczone będą wraz z urządzeniami i w języku polskim (lub za zgodą Zamawiającego w języku angielskim)."
Zwracamy się z prośbą o udzielenie zgody na dostarczenie instrukcji producenta w języku angielskim.

Odpowiedź:
Zamawiający dokonuje zmiany treści § 3 ust. 6 SIWZ Załącznika nr 8.2 do SIWZ, nadając mu brzmienie:
„Wykonawca zapewnia, ze wszelkie instrukcje niezbędne do wykorzystania dostarczonego przedmiotu umowy przez użytkowników Zamawiającego, dostarczone będą wraz z urządzeniami i w języku polskim lub angielskim".

Pytanie 29:
Dotyczy wymagania: Rozdział VIII SIWZ, pkt. 3) a)
„... Zamawiający dopuszcza możliwość posługiwania się wydrukami ze stron internetowych producenta ... „
Czy wymaganie zostanie uznane za spełnione, jeśli Dostawca dostarczy dokumenty producenta, pobrane ze stron internetowych producenta, w języku angielskim ?

Odpowiedź:

Zamawiający informuje, że w Rozdziale VIII pkt 3 a) SIWZ nie ma takiego zapisu, pytanie zapewne dotyczy zapisu Rozdziału IX ust. 3 pkt 3 lit. a) i zgodnie z informacją zawartą w SIWZ w tym punkcie: *„dokumenty w języku obcym, składane są wraz z tłumaczeniem na język polski".*

Pytanie 30:
Dotyczy wymagania nr 4 z załącznika nr 2.1

Czy Zamawiający dopuści rozwiązanie obsługujące nie mniej niż 3 000 000 jednoczesnych połączeń zamiast „4 000 000" jednoczesnych połączeń?

Odpowiedź:
Zamawiający dokonał zmiany poz. 4 poprzez zmianę wymagania dot. liczby jednoczesnych połączeń:
„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 anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 3 000 000 jednoczesnych połączeń"
Liczba jednoczesnych połączeń wyższa niż 3 000 000 została ustanowiona kryterium oceny ofert:
„Ilość połączeń <4000000 – 0 pkt;
Ilość połączeń ≥4000000 – 5 pkt"

Pytanie 31:
Dotyczy wymagania nr 5 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie posiadające 8 portów Ethernet 1 GbE RJ45, 12 portów 1 GbE SFP, 4 porty 10 GbE SFP+ zamiast „4 porty Ethernet 100M/1G/10G, 16 portów 1G/10G SFP/SFP+, 4 porty 40G QSFP+". Proszę podać ilość i typ wkładek SFP/SFP+, które należy uwzględnić w wycenie.

Odpowiedź:
Zamawiający udzielił odpowiedzi powyżej – odpowiedź na pytanie 1.

Pytanie 32:
Dotyczy wymagania nr 9 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie bez wsparcia dla wirtualnych routerów?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 3.

Pytanie 33:
Dotyczy wymagania nr 15 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym definiowanie kontroli aplikacji odbywa się w osobnym profilu (application firewall) niż podstawowa polityka firewall?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 13 Załącznika nr 2.1 do SIWZ.

Pytanie 34:
Dotyczy wymagania nr 20 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie bez możliwości tworzenia oddzielnych profili ochrony per aplikacja, ale umożliwia tworzenie wyjątków dla poszczególnych aplikacji i granularnie, dla każdej z sygnatur danej aplikacji?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 4.

Pytanie 35:
Dotyczy wymagania nr 21 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie posiadające ponad 167 sygnatur dla różnych typów plików z możliwością tworzenia własnych sygnatur aplikacji (samodzielnie lub z pomocą producenta). Zamknięta lista plików faworyzuje jednego producenta.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 5.

Pytanie 36:
Dotyczy wymagania nr 23 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie posiadające możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla wybranych kategorii stron określonych polityką bezpieczeństwa? Wyświetlanie akcji „kontynuuj" dla funkcji blokowania transmisji plików faworyzuje rozwiązanie jednego producenta.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 6.

Pytanie 37:
Dotyczy wymagania nr 31 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie posiadające możliwość realizacji SSO z systemami Linux/MacOS w oparciu o protokół Samba oraz NetAPI? Mechanizm umożliwia automatyczne uwierzytelnianie użytkowników jednak w dużo bardziej wydajny sposób niż analiza danych syslog.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 8.

Pytanie 38:
Dotyczy wymagania nr 33 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które nie ma możliwości usunięcia zawartości pola x-forwarded-for z pakietu? Funkcja ta jest praktycznie bezużyteczna ponieważ większość systemów IPS/IDS zablokuje pakiet z pustym polem XFF.

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 28 Załącznika nr 2.1 do SIWZ.

Pytanie 39:
Dotyczy wymagania nr 38 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym moduł inspekcji antywirusowej uruchamia się per strefa bezpieczeństwa, a nie aplikacja, ale moduł inspekcji antywirusowej posiada możliwość tworzenia wyjątków per obiekt adresowy lub jest możliwość wyłączenia inspekcji antywirusowej per polityka bezpieczeństwa firewall?

Odpowiedź:
Zamawiający ustanowił spełnienie wymagań z poz. 38 warunkiem fakultatywnym, umożliwiającym uzyskanie punktów w kryterium oceny ofert. Powyższe informacje zawiera obecnie poz. 101 Załącznika nr 2.1 do SIWZ.

Pytanie 40:
Dotyczy wymagania nr 39 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym moduł inspekcji antywirusowej uruchamia się per strefa bezpieczeństwa, ale jest możliwość wyłączenia tej inspekcji per polityka bezpieczeństwa firewall?

Odpowiedź:

Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 32 Załącznika nr 2.1 do SIWZ

Pytanie 41:
Dotyczy wymagania nr 41 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym moduł IPS/IDS uruchamia się per strefa bezpieczeństwa, ale jest możliwość wyłączenia tej inspekcji per polityka bezpieczeństwa firewall?

Odpowiedź:

Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 34 Załącznika nr 2.1 do SIWZ

Pytanie 42:
Dotyczy wymagania nr 44 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym moduł anty-spyware uruchamia się per strefa bezpieczeństwa, ale jest możliwość wyłączenia tej inspekcji per polityka bezpieczeństwa firewall?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 37 Załącznika nr 2.1 do SIWZ

Pytanie 43:
Dotyczy wymagania nr 45 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie bez możliwości tworzenia sygnatur anty-spyware na urządzeniu, ale z możliwością tworzenia sygnatur w module kontroli aplikacji np. za pomocą wyrażeń „regex" oraz z pomocą wsparcia producenta?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 11.

Pytanie 44:
Dotyczy wymagania nr 46 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązane realizujące tą funkcjonalność jako filtr Botnet blokujący ruch do domen uznanych za złośliwe?

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 38 Załącznika nr 2.1 do SIWZ.

Pytanie 45:
Dotyczy wymagania nr 47 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie bez możliwości podmiany adresu IP w odpowiedziach DNS? Identyfikacja hostów zarażonych odbywa się na podstawie informacji z modułu Botnet i korelacji tych danych z adresem IP hosta.

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 39 Załącznika nr 2.1 do SIWZ.

Pytanie 46:
Dotyczy wymagania nr 50 z załącznika nr 2.1
Czy Zamawiający dopuści zastosowanie rozwiązania, które umożliwia wyświetlenie komunikatu do zaakceptowania przez użytkownika z informacją o nie podawaniu poświadczeń podczas wchodzenia na strony z określonej kategorii?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 12.

Pytanie 47:
Dotyczy wymagania nr 51 z załącznika nr 2.1
Czy Zamawiający dopuszcza zastosowanie rozwiązania, które nie ma możliwości wykrywania sieci botnet na podstawie analizy behawioralnej, ale posiada możliwość współpracy z systemami SIEM, które posiadają taką możliwość.

Odpowiedź:

Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 43 Załącznika nr 2.1 do SIWZ

Pytanie 48:
Dotyczy wymagania nr 52 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które ma możliwość analizy plików: wykonywalnych, PDF, Office oraz archiwów bez możliwości rozdzielania dla poszczególnych aplikacji czy wyboru kierunku? Czy w ofercie powinna zostać uwzględniona licencja na funkcjonalność sandbox?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 13.

Pytanie 49:
Dotyczy wymagania nr 57 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym połączenia SSL VPN oraz Ipsec VPN dla użytkowników (client to site) są licencjonowane, ale nie ma potrzeby zakupu licencji na aplikację kliencką? Jest to bardziej efektywna forma licencjonowania ponieważ można posiadać
np. 10 licencji na jednoczesne połączenia SSL VPN i np. 100 użytkowników będzie mogło mieć zainstalowaną aplikację kliencką.

Odpowiedź:
Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 49 Załącznika nr 2.1 do SIWZ.

Pytanie 50:
Dotyczy wymagania nr 58 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie w którym istnieje możliwość inspekcji ruchu GRE lub nieszyfrowanym IPSec mechanizmami: IPS, antywirus, antyspyware, kontrola aplikacji ? (bez QoS i DoS). Wymaganie wskazuje na jednego producenta.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 14.

Pytanie 51:
Dotyczy wymagania nr 59 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które wykorzystuje mechanizmy RADIUS lub LDAP (bez TACACS+, Kerberos, SAML 2.0).

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 15.

Pytanie 52:
Dotyczy wymagania nr 63 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które nie posiada integracji z środowiskiem Vmware w przedstawiony sposób, natomiast umożliwia budowanie polityk firewall z wykorzystaniem adresów fizycznych.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 16.

Pytanie 53:
Dotyczy wymagania nr 65 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które realizuje tą funkcjonalność na dedykowanej platformie do zarządzania?

Odpowiedź:

Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 53 Załącznika nr 2.1 do SIWZ.

Pytanie 54:
Dotyczy wymagania nr 66 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które posiada moduł zarządzanie zmianą (akceptowanie zmian od różnych administratorów) na dedykowanej platformie do zarządzania?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 17.

Pytanie 55:
Dotyczy wymagania nr 68 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie posiadające REST API?

Odpowiedź:

Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 19.

Pytanie 56:
Dotyczy wymagania nr 70 z załącznika nr 2.1
Czy Zamawiający jest w stanie zrezygnować z uwierzytelniania za pomocą TACACS+ i Kerberos?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 20.

Pytanie 57:
Dotyczy wymagania nr 71 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które umożliwia stworzenie sekwencji uwierzytelniającej składającej się z dwóch metod?

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 21.

Pytanie 58:
Dotyczy wymagania nr 72 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie, które wyposażone jest w dwa dyski 80 GB SSD. Logi pochodzące z firewall'a i tak będą przechowywane na zewnętrznej platformie do zarządzania i raportowania.

Odpowiedź:

Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 22.

Pytanie 59:
Dotyczy wymagania nr 74 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie bez możliwości sprawdzenia wpływu sygnatur na polityki bezpieczeństwa? Taka konfiguracja wymagałaby manualnej aktualizacji sygnatur i jest dużo wolniejsza od automatycznej aktualizacji.

Odpowiedź:
Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 23.

Pytanie 60:
Dotyczy wymagania nr 75 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie pozwalające na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per atrybut logowania, ale bez podziału na oddzielne polityki bezpieczeństwa?

Odpowiedź:

Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 24.

Pytanie 61:
Dotyczy wymagania nr 77 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie bez możliwości „generowania zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.". Taką funkcjonalność można zrealizować z wykorzystaniem zewnętrznego serwera bez obciążania firewall'a dodatkowymi zadaniami związanymi z raportowaniem.

Odpowiedź:

Zamawiający odpowiedział na pytanie powyżej – odpowiedź na pytanie 25.

Pytanie 62:
Dotyczy wymagania nr 79 z załącznika nr 2.1
Czy Zamawiający dopuści rozwiązanie posiadające wymaganą funkcjonalność z wykorzystaniem zewnętrznej platformy raportowania dostarczonej z urządzeniem firewall w postaci maszyny wirtualnej z pominięciem raportów w formacie XML?

Odpowiedź:

Zamawiający wymaga, aby funkcjonalność z poz. 79 (obecnie poz. 65) była również realizowana przez urządzenie firewall. Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 65 Załącznika nr 2.1 do SIWZ.

Pytanie 63:
Dotyczy wymagania nr 81 z załącznika nr 2.1
Czy Zamawiający wymaga licencji umożliwiającej konfigurację klastra Active-Active czy licencje na klaster Active-Passive są wystarczające?

Odpowiedź:

Zamawiający pozostawia zapisy SIWZ w powyższym zakresie bez zmian. Powyższy zapis stanowi obecnie poz. 67 Załącznika nr 2.1 do SIWZ

Pytanie 64:
Dotyczy wymagania nr 83 z załącznika nr 2.1
Czy Zamawiający wymaga dostarczenia licencji do zarządzania, logowania i raportowania dla 25 firewalli czy licencje na podłączenie systemów firewall będących przedmiotem tego postępowania będą wystarczające?

Odpowiedź:
Zamawiający wymaga zaoferowania jedynie licencji na podłączenie systemów firewall będących przedmiotem tego postępowania.

Zamawiający informuje, że dokonał zmiany Formularza wymaganych warunków technicznych w zakresie Pakietu 1, stanowiącego Załącznik nr 2.1 do SIWZ, poprzez zmianę parametrów technicznych.

Zmieniony **Załącznik nr 2.1 oraz nr 8.2** Zamawiający zamieścił na stronie internetowej www.wum.edu.pl

Zamawiający dokonał również zmiany treści SIWZ w zakresie kryterium oceny ofert. W związku z powyższym Rozdział SIWZ otrzymuje brzmienie:

XIV. KRYTERIA OCENY OFERT ORAZ ICH ZNACZENIE ORAZ SPOSÓB OCENY OFERT

1. **Kryteria oceny ofert i ich znaczenie:**

Pakiet 1:	**Pakiet 2 i 3:**
Cena – 40%; **Gwarancja – 10%;** **Ocena techniczna – 50%;**	**Cena – 80%;** **Gwarancja – 10%;** **Ocena techniczna – 10%;**

Za najkorzystniejszą ofertę zostanie uznana oferta która uzyska największa liczbę punktów obliczaną wg wzoru:

$$\mathbf{K = K_C + K_G + K_{OT}}$$

gdzie:
K – liczba punktów oferty ocenianej
K_C – liczba punktów przyznanych ofercie ocenianej w kryterium „Cena"
K_G – liczba punktów przyznanych ofercie ocenianej w kryterium „Gwarancja"
K_{OT} – liczba punktów przyznanych ofercie ocenianej w kryterium „Ocena techniczna"

2. **Kryteria oceny ofert, Pakiet 1:**

1) **W kryterium ceny (Kc) – 40%**

Zamawiający każdej z ofert przyzna liczbę punktów obliczoną wg wzoru:

$K_C = (C_{min} / C_C) \times 40\% \times 100$

gdzie:

K_C – liczba punktów przyznanych ocenianej ofercie w kryterium „Cena"
C_{min} – najniższa zaoferowana cena (brutto)
C_C – cena oferty ocenianej
100 – współczynnik stały

2) **W kryterium gwarancja (K_G) – 10%**

Zamawiający każdej ofercie ocenianej, której okres gwarancji spełnia warunki określone w Rozdziale V przyzna po 5 punktów (nie więcej niż 10 punktów) **za każde pełne 12 miesięcy** powyżej okresu gwarancji określonego w Rozdziale V jako minimalny.
W przypadku nie wpisania przez Wykonawcę zaoferowanego okresu gwarancji, Zamawiający przyjmie, że został zaoferowany minimalny wymagany termin i przyzna ofercie w kryterium „Gwarancja" 0 pkt.

3) **W kryterium ocena techniczna (K_{OT}) – 50 %,**

W kryterium „Ocena techniczna" Zamawiający przyzna liczbę punktów obliczoną wg wzoru:

$\mathbf{K_{OT}} = (K_O / K_{max}) \times 50\% \times 100$

gdzie:

K_{OT} – liczba punktów przyznanych ocenianej ofercie w kryterium „Ocena techniczna"
K_O – łączna liczba punktów cząstkowych oferty ocenianej, obliczona wg wzoru: $\mathbf{K_O} = P_{T1} + P_{T2}$ wyszczególnionych w Załączniku 2.1 do SIWZ
K_{max} – największa łączna liczba punktów cząstkowych możliwych do uzyskania w tym kryterium
100 – współczynnik stały

Punkty cząstkowe (P_{T1} i P_{T2}) Zamawiający przyzna wg następujących zasad:

Parametr oceniany		Liczba punktów
Pakiet 1		
P_{T1}	System zabezpieczeń firewall musi obsługiwać nie mniej niż 3 000 000 jednoczesnych połączeń	Ilość połączeń <4000000 – 0 pkt Ilość połączeń ≥4000000 – 5 pkt
P_{T2}	System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.	Nie – 0 pkt Tak – 5 pkt
P_{T3}	System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików mdi, ocx, sh	Nie – 0 pkt Tak – 5 pkt
P_{T4}	System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.	Nie – 0 pkt Tak – 5 pkt
P_{T5}	System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.	Nie – 0 pkt Tak – 5 pkt
P_{T6}	System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.	Nie – 0 pkt Tak – 5 pkt
P_{T7}	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.	Nie – 0 pkt Tak – 5 pkt
P_{T8}	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	Nie – 0 pkt Tak – 5 pkt

P_{T9}	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.	Nie – 0 pkt Tak – 5 pkt
P_{T10}	System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.	Nie – 0 pkt Tak – 5 pkt
P_{T11}	System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.	Nie – 0 pkt Tak – 5 pkt
P_{T12}	System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.	Nie – 0 pkt Tak – 5 pkt
P_{T13}	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	Nie – 0 pkt Tak – 5 pkt
P_{T14}	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.	Nie – 0 pkt Tak – 5 pkt
P_{T15}	System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych	Nie – 0 pkt Tak – 5 pkt

	AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.	
P_{T16}	System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.	Nie – 0 pkt Tak – 5 pkt
P_{T17}	System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.	Nie – 0 pkt Tak – 5 pkt

3. **Kryteria oceny ofert, Pakiet 2 i 3:**

1) **W kryterium ceny (Kc) – 80%**

Zamawiający każdej z ofert przyzna liczbę punktów obliczoną wg wzoru:

$K_C = (C_{min} / C_C) \times 80\% \times 100$

gdzie:

K_C – liczba punktów przyznanych ocenianej ofercie w kryterium „Cena"
C_{min} – najniższa zaoferowana cena (brutto)
C_C – cena oferty ocenianej
100 – współczynnik stały

2) **W kryterium gwarancja (K_G) – 10%**

Zamawiający każdej ofercie ocenianej, której okres gwarancji spełnia warunki określone w Rozdziale V przyzna po 5 punktów (nie więcej niż 10 punktów) **za każde pełne 12 miesięcy** powyżej okresu gwarancji określonego w Rozdziale V jako minimalny.
W przypadku nie wpisania przez Wykonawcę zaoferowanego okresu gwarancji, Zamawiający przyjmie, że został zaoferowany minimalny wymagany termin i przyzna ofercie w kryterium „Gwarancja" 0 pkt.

3) **W kryterium ocena techniczna (K_{OT}) – 10 %,**

W kryterium „Ocena techniczna" Zamawiający przyzna liczbę punktów obliczoną wg wzoru:

$K_{OT} = (K_O / K_{max}) \times 10\% \times 100$

gdzie:

K_{OT} – liczba punktów przyznanych ocenianej ofercie w kryterium „Ocena techniczna"

K_O – łączna liczba punktów cząstkowych oferty ocenianej, obliczona wg wzoru: $K_O = P_{T1} + P_{T2}$ wyszczególnionych odpowiednio dla Pakietu w Załącznikach 2.2 – 2.3 do SIWZ

K_{max} – największa łączna liczba punktów cząstkowych możliwych do uzyskania w tym kryterium

100 – współczynnik stały

Punkty cząstkowe (P_{T1} i P_{T2}) Zamawiający przyzna wg następujących zasad:

Parametr oceniany		**Liczba punktów**
Pakiet 2		
P_{T1}	Wydajność poprawnego ruchu	≥1< 2 Gbps – 0 pkt ≥ 2 Gbps – 5 pkt
P_{T2}	Wydajność blokowania ataków DDoS Flood:	≥1< 2 mln pps – 0 pkt ≥ 2 mln pps – 5 pkt
Pakiet 3		
P_{T1}	Przepustowość	571 mln pps - 0 pkt >571 mln pps - 5 pkt

4. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym ofert dodatkowych.

Zamawiający informuje, że zmienia termin składania ofert na dzień 31.08.2017 r. do godziny 09:30. Otwarcie ofert nastąpi w dniu 31.08.2017 r. o godzinie 10:00.
Miejsce składania i otwarcia ofert pozostają bez zmian.

Z poważaniem

Łukasz Szlachetka
Przewodniczący Komisji Przetargowej

ul. Żwirki i Wigury 61, 02-091 Warszawa
tel.: 0-22 57-20-373, faks: 0-22 57-20-331
e-mail: elzbieta.jakoniuk@wum.edu.pl
www.wum.edu.pl