Warszawa, dnia 25.01.2022 r.

DZP-361/147/2021/AZ/91

**Do wszystkich zainteresowanych**

Dotyczy przetargu nieograniczonego nr DZP-361/147/2021 pn: „Zakup firewalla na potrzeby Centrum Przetwarzania Danych UW”.

Informujemy, że do Zamawiającego wpłynęły od Wykonawcy zapytania. Zamawiający na podstawie art. 135 ustawy Prawo zamówień publicznych, zwanej dalej ustawą udziela odpowiedzi oraz na podstawie art. 137 ust. 1 ustawy zmienia treść Specyfikacji Warunków Zamówienia, zwanej dalej SWZ.

**Zestaw nr 1**

**Pytanie 1**. W poszczególnych punktach wymagań Zamawiający wskazuje, że poszczególne funkcje firewalla są z jednej strony wymagane z drugiej zaś strony określone jako te, które powinny pojawić się w ramach „możliwości rozbudowy” Przykładowe w p. II.A.10 Zamawiający wskazuje wymagania dla IPS, antywirus i antyspyware jako, te które należy przewidzieć w ramach opcji rozbudowy, natomiast już w p. II.A.13 funkcje te są wymagane przy realizacji inspekcji po deszyfracji HTTPS. Podobnie w p. II.A.15. Wnosimy zatem ponowne przeanalizowanie wymagań dotyczących silników inspekcyjnych opisanych wp.II.A.9 do II.A.15 i informację, które z nich powinny zostać uwzględnione przez Wykonawców w ofertach.

**Odpowiedź Zamawiającego:**

Odpowiadając na pytanie Zamawiający na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w zakresie Załącznika nr 1 do SWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA.

Nowe brzmienie punktu II.A.9: Firewall musi zapewnić funkcjonalność analizy plików wykonywalnych (exe, dll) przechodzących przez firewall współpracując z zewnętrznym systemem utrzymywanym przez producenta w Internecie, który instaluje i uruchamia przesłane pliki w wirtualnym środowisku oraz sprawdza czy dany plik nie zachowuje się w złośliwy sposób (np. kasuje lub zaraża inne pliki, zmienia ustawienia komputera, nawiązuje komunikację zwrotną, otwiera porty, zmienia ustawienia usług systemowych, itp). System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.

Nowe brzmienie punktu II.A.10: Możliwość rozbudowy (wyłącznie w oparciu o zakup licencji) o funkcjonalność filtrowania stron WWW (WWW/URL Filtering) w zależności od predefiniowanych kategorii. Baza stron WWW musi zawierać nie mniej niż 200 milionów rekordów URL oraz zapewniać możliwość kategoryzacji stron i określać ich poziom bezpieczeństwa (co najmniej trzystopniowo tj. poziom wysoki-średni-niski)

Nowe brzmienie punktu II.A.11: Firewall musi zapewnić funkcjonalność wykrywania i blokowania ruchu do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

Nowe brzmienie punktu II.A.15: Firewall musi zapewnić funkcjonalność inspekcji ruchu modułami IDS/IPS, AntiSpyware, AntiVirus, DLP bez konieczności dokupowania jakichkolwiek dodatkowych komponentów. Bazy sygnatur muszą być przechowywane na urządzeniu, regularnie aktualizowane w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduły inspekcji muszą być uruchamiane niezależnie per reguła polityki bezpieczeństwa. Nie jest dopuszczalne, aby moduły uruchamiane były per cały firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).

Nowe brzmienie punktu II.B.23.5: aktualizację silników i baz sygnatur modułów bezpieczeństwa (czas liczony jak w punkcie II.B.22),

**Pytanie 2**. W punkcie II.A.13 Zamawiający wskazał, że wymaga inspekcji szyfrowanej komunikacji HTTPS/SSL. Czy Zamawiający może potwierdzić, że posługując się parasolowym terminem SSL ma na myśli de facto protokoły SSL 3.0, TLS 1.0, TLS 1.2 I TLS 1.3 I że wymaga, aby firewall posiadał możliwość deszyfracji w/w protokołów I analizy danych aplikacyjnych celem szczegółowej identyfikacji aplikacji I zastosowania inspekcji bezpieczeństwa?

**Odpowiedź Zamawiającego:**

Odpowiadając na pytanie Zamawiający na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w zakresie Załącznika nr 1 do SWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA.

Nowe brzmienie punktu II.A.13: Firewall musi umożliwiać inspekcję komunikacji szyfrowanej (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) dla ruchu wychodzącego i przychodzącego. Firewall musi umożliwiać deszyfrację wskazanego ruchu HTTPS (szyfrowanego 3DES, AES (128-bit, 192-bit, 256-bit)) i poddania go właściwej inspekcji nie mniej niż: identyfikacja aplikacji, wykrywanie i blokowanie ataków typu exploit (Intrusion Prevention - IPS), wirusy i inny złośliwy kod (AntiVirus i AntiSpyware).

**Pytanie 3**. W punkcie II.B.10 Zamawiający określił, iż wymaga, aby system firewall zapewniał możliwość weryfikacji kondycji bezpieczeństwa stacji roboczej przed podłączeniem jej do VPN. W przypadku większości rozwiązań na rynku taka weryfikacja odbywa się z wykorzystaniem bądź klienta VPN oferowanego przez producenta systemu firewall lub też z wykorzystaniem dedykowanego agenta. Czy Zamawiający dopuści zastosowanie systemu, w którym określenie kondycji bezpieczeństwa hosta dołączanego do sieci VPN będzie odbywało się z wykorzystaniem dodatkowego oprogramowania na stacji końcowej?

**Odpowiedź Zamawiającego:**

Odpowiadając na pytanie Zamawiający na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w zakresie Załącznika nr 1 do SWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA.

Nowe brzmienie punktu II.B.10: Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej (co najmniej dla Windows) co najmniej w zakresie obecności oprogramowania antywirusowego, przynależności do domeny Active Directory i stanu lokalnego firewalla. Określenie kondycji bezpieczeństwa może odbywać się z wykorzystaniem zainstalowanego klienta VPN dostarczonego przez producenta urządzenia.

**Pytanie 4**. W punkcie II.B.10 Zamawiający określił, iż wymaga, aby system firewall zapewniał możliwość weryfikacji kondycji bezpieczeństwa stacji roboczej przed podłączeniem jej do VPN. W przypadku większości rozwiązań na rynku taka weryfikacja odbywa się z wykorzystaniem bądź klienta VPN oferowanego przez producenta systemu firewall lub też z wykorzystaniem dedykowanego agenta. Czy właściwym jest rozumienie, iż oprogramowanie klienta VPN oraz agenta należy przewidzieć dla 2000 użytkowników – względem maksymalnej liczby jednoczesnych sesji opisanej w p. II.C.10.3

**Odpowiedź Zamawiającego:**

Zamawiający musi mieć możliwość zainstalowania klienta VPN, na urządzeniach wszystkich pracowników - co najmniej 10 000 urządzeń, przy czym liczba jednocześnie podłączonych do VPN urządzeń nie przekroczy 2 000.

**Pytanie 5** W punkcie II.B.17 Zamawiający określił, iż wymaga edycji konfiguracji bez jej jednoczesnego aplikowania. Jednocześnie Zamawiający pozostawił tutaj bardzo duże pole do interpretacji, gdyż w skrajnym przypadku formą edycji konfiguracji może być wgranie nowego pliku konfiguracyjnego i wskazanie go jako konfiguracji domyślnej po restarcie urządzenia. Stąd też prosimy o wyjaśnienie jak należy literalnie rozumieć to wymaganie.

**Odpowiedź Zamawiającego:**

Zmiany konfiguracji wprowadzone przez administratora w panelu zarządzania (CLI lub GUI) nie będą aplikowane na urządzeniu w momencie dokonywania zmiany, a dopiero po zleceniu ich aplikacji. Administrator musi mieć możliwość: podglądu jakie zmiany zostaną wprowadzone, wycofania zmian, zapisania zmian oraz aplikacji zmian w zaplanowanym czasie. Dodatkowo urządzenie musi zapewniać możliwość porównania konfiguracji co najmniej pomiędzy 50 ostatnimi zleconymi zmianami. Wymienione wyżej funkcje muszą być dostępne bezpośrednio na urządzeniu.

**Pytanie 6.** W punkcie II.C.9 Zamawiający określił, iż wymaga, aby dostarczone urządzenie zapewniło możliwość obsługi 2,3 mln jednoczesnych sesji. Czy Zamawiający dopuści rozwiązania, które spełnia wszystkie wskazane przez Zamawiającego funkcje i parametry wydajnościowe, jednakże będzie posiadało możliwość obsługi 2.2 mln jednoczesnych sesji. Zwracamy się z prośbą o uwzględnienie możliwości zaoferowania takiego urządzenia – różnica w liczbie obsługiwanych sesji jest relatywnie niewielka (mniej niż 5%), a jednocześnie zaproponowanie urządzenia ”większego” spowoduje około 50% wzrost ceny oferty.

**Odpowiedź Zamawiającego:**

Odpowiadając na pytanie Zamawiający na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w zakresie Załącznika nr 1 do SWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA.

Nowe brzmienie punktu II.C.9: Firewall musi obsługiwać co najmniej 2,2 mln jednoczesnych sesji.

**Pytanie 7.** W punkcie III Zamawiający określił wymagania dla systemu zarządzającego.

Jednocześnie Zamawiający w żaden sposób nie określa ani formy (dedykowany appliance, maszyna wirtualna) w jakiej system zarządzania powinien zostać dostarczony (chociaż zapis w p. III.B może sugerować, że Zamawiający oczekuje systemu w postaci maszyny wirtualnej, to jednak w żaden sposób wymaganie takie nie zostało wyartykułowane), ani parametrów wydajnościowych i skalowania - co pozwala na bardzo dużą swobodę interpretacji przez Wykonawców.

Systemy te różnią się również obsługiwaną przestrzenią na logi i w skrajnej sytuacji Wykonawca może zaoferować system obsługujący niewielki wolumen logów – który przykładowo zostanie zapełniony przez okres 1-2 tygodni -tym samym może okazać się, że taki system jest dla Zamawiającego bezużyteczny i/lub będzie wymagać kosztowej rozbudowy. Biorąc zatem pod uwagę różnorodność systemów zarządzania wnosimy o doszczegółowienie specyfikacji, co pozwoli na złożenie oferty spełniającej oczekiwania Zamawiającego. Prosimy o wskazanie, jakich cech i funkcji Zamawiający oczekuje od systemu zarządzania oraz jaki wolumen logów powinno to rozwiązanie obsłużyć i jaką przestrzeń dyskową zapewniać na te logi.

**Odpowiedź Zamawiającego:**

Wydajność i przestrzeń dyskowa na logi powinna być zależna od przydzielonych zasobów i wydajności środowiska wirtualnego Zamawiającego.

Nowe brzmienie pkt III.A.2: Zbieranie i analizowanie logów (w ramach dostarczonej licencji system musi zapewnić co najmniej 8TB przestrzeni dyskowej na logi)

Nowe brzmienie pkt III.B: Platforma powinna zostać dostarczona jako licencja na maszynę wirtualną zgodną ze środowiskiem wirtualizacji VMware ESXi 6.7 i nowszym

**Pytanie 8**. W Załączniku nr 2 – projektowane postanowienia umowy w par.6 Zamawiający określił zapisy umowy dotyczące świadczenia serwisu gwarancyjnego. Uprzejmie prosimy o potwierdzenie, iż w ramach realizacji umowy Zamawiający nie będzie wymagał od Wykonawcy by pozostawił uszkodzone nośniki danych u Zamawiającego?

**Odpowiedź Zamawiającego:**

W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki muszą pozostać w całości u Zamawiającego.

**Pytanie 9.** Dotyczy opisu kryteriów oceny ofert, gdzie Zamawiający określa, iż przyzna 15 punktów za dostawę urządzeń, których średni czas bezawaryjnej pracy (MTBF) będzie na poziomie 20 lat. Wnosimy o rozważenie skrócenia czasu MTBF, za który Wykonawca otrzyma maksymalną punktację do 15 lat. Jako Wykonawca pragniemy wskazać, iż urządzenia firewall w odróżnieniu od innych urządzeń sieciowych mają krótszy czas życia. Wynika, to m.in. z tego, że wartością urządzeń bezpieczeństwa jest w głównej części oprogramowanie i częstotliwość oraz jakość uaktualnień dotyczących zagrożeń powiązana z tym oprogramowaniem – zgodnie z wymaganiami z OPZ te uaktualnienia muszą być przesyłane codziennie. Z drugiej strony urządzenia sieciowe takie jak routery czy przełączniki niejednokrotnie działają miesiącami czy latami bez aktualizacji.

Dlatego też w przypadku firewalli cykl, iż życia jest kluczowy – w przypadku dominującej części producentów wynosi on 10-13 lat. Przykładowo urządzenia o parametrach wydajnościowych zbliżonych do wymaganych przez Zamawiającego:

* Produkcji Cisco – model ASA 5585-X produkowany był przez 8 lat (od 2010) i przez kolejnych 5 lat będzie wspierany po zakończeniu sprzedaży
* Produkcji Cisco – model Firepower 4110 produkowany był przez 4 lata (od 2016) i przez kolejnych 5 lat wspierany po zakończeniu sprzedaży
* Produkcji Checkpoint – modele serii 15x00 oferowane były przez 5 lat – od stycznia 2016 do grudnia 2020 – są wspierane przez kolejnych 5 lat od daty zakończenia sprzedaży
* Produkcji Checkpoint – modele serii 23x00 oferowane były przez 5 lat – od stycznia 2016 do grudnia 2020 – są wspierane przez kolejnych 5 lat od daty zakończenia sprzedaży
* Produkcji Palo Alto – modele serii 5000 dostępne były przez 8 lat (2011-2019) i przez 5 lat będą wspierane przez producenta
* Produkcji Palo Alto – modele serii 3000 dostępne były przez 7 lat (2012-2019) i przez 5 lat będą wspierane przez producenta

Powyższe wskazuje, iż najdłużej dostępne rozwiązania funkcjonowały na rynku przez 13 lat, a podobną politykę prowadzą praktycznie wszyscy dostawcy firewalli.

Jednocześnie firewalle, które nie są już wspierane przez producentów tracą ogromną część swojej wartości technicznej, przez co niezmiernie trudno znaleźć użytkowników korzystających z urządzeń firewall wdrażanych 20 lat temu i nadal produkcyjnie wykorzystywanych. Przyjęcie czasu 15 lat jest uzasadnione technologicznie, gdyż jest on realnym odzwierciedleniem maksymalnego okresu użytkowania urządzeń.

Podawanie przez Wykonawców czasu maksymalnego – 20 lat - nie będzie w żaden sposób

uzasadnione technologicznie a jedynie pozwoli na uzyskanie dodatkowych punktów. Oczywistym jest bowiem to po upływie okresu 10-13 lat należy oczekiwać, iż urządzenia będą technologicznie zastępowane nowymi generacjami, a brak wsparcia producentów dla starszych modeli będzie powodował ich bezużyteczność względem stawianych im wymagań. Wnosimy zatem o rozważenie możliwości zmiany kryterium oceny oferty dotyczącego średniego czasu bezawaryjnej pracy na 15 lat lub potwierdzenie podtrzymania kryterium w formie i wagach opisanych w SWZ.

**Odpowiedź Zamawianego:**

Zamawiający przychyla się do prośby i zmienia maksymalny parametr kryterium oceny oferty dotyczący średniego czasu bezawaryjnej pracy na 15 lat.

**Pytanie 10.** Dotyczy opisu kryteriów oceny ofert, gdzie Zamawiający określa, iż przyzna 15 punktów za dostawę urządzeń, których średni czas bezawaryjnej pracy (MTBF) będzie na poziomie 20 lat. Jakich środków dowodowych Zamawiający wymaga dla potwierdzenia spełnienia wymagania opisanego w tym kryterium? Czy Zamawiający dopuści jako środek dowodowy oświadczenie producenta lub polskiego jego przedstawicielstwa?

**Odpowiedź Zamawiającego:**

Zamawiający nie dopuści oświadczenia producenta lub polskiego przedstawiciela. W przypadku zadeklarowania spełnienia kryterium „Czas bezawaryjnej pracy (MTBF)” Wykonawca, musi wykazać spełnienie tego wymagania w publicznie dostępnej dokumentacji technicznej (poprzez dostarczenie karty katalogowej lub wskazanie odnośnika do oficjalnej strony producenta) oferowanego urządzenia.

**Pytanie 11**. Dotyczy punktu II.C.4 Do firewalla muszą być dołączone 4 współpracujące z nim interfejsy optyczne pracujące w standardzie 10GBASE-SX SFP+ oraz 4 współpracujące z nim interfejsy optyczne pracujące w standardzie 40GBASE-SR QSFP+.

Czy Zamawiający wyrazi zgodę na dostarczenie modułów optycznych pracujących w standardzie 10GBASE-SR SFP+ zamiast 10GBASE-SX SFP+ ?

**Odpowiedź Zamawiającego:**

Odpowiadając na pytanie Zamawiający na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w zakresie Załącznika nr 1 do SWZ – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA.

Nowe brzmienie punktu II.C.4:

Do firewalla muszą być dołączone 4 współpracujące z nim interfejsy optyczne pracujące w standardzie 10GBASE-SR SFP+ oraz 4 współpracujące z nim interfejsy optyczne pracujące w standardzie 40GBASE-SR QSFP+:

**Zestaw nr 2**

„Zamawiający wskazuje w Załączniku nr 1 – SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

– SPECYFIKACJA TECHNICZNA. System zabezpieczeń ruchu sieciowego:

II.C Wymagania wydajnościowe

II.C.1 Firewall musi być dostarczony jako dedykowane urządzenie typu appliance z dedykowanym dla niego oprogramowaniem systemowym. Obudowa wraz z kompletem mocowań umożliwiających montaż w szafie rack 19” i zajmować maksymalnie 2 RU. Całość sprzętu i oprogramowania musi pochodzić od jednego producenta.

Wykonawca zwraca się z pytaniem: Czy Zamawiający dopuszcza rozwiązanie spełniające wymogi OPZ oparte na komponentach mniejszych niż 2U i zgodnie z wymaganiami całość systemu nie przekraczająca 4U.”

**Odpowiedź Zamawiającego:**

Zamawiający nie wyraża zgody.

Ponadto Zamawiający na podstawie art. 137 ust. 1 ustawy dokonuje zmiany treści SWZ w zakresie opisu kryteriów i sposób oceny ofert.

Nowe brzmienie art. 10 § 1 ust. 1 pkt. 3 SWZ:

1. **Czas bezawaryjnej pracy (MTBF) /P/** - czas bezawaryjnej pracy (MTBF) dla zaproponowanych

urządzeń deklarowany przez producenta i wpisany przez Wykonawcę do Formularza oferty, liczony w pełnych latach.

Wykonawca, musi wykazać spełnienie tego wymagania w publicznie dostępnej dokumentacji technicznej (poprzez dostarczenie karty katalogowej lub wskazanie odnośnika do oficjalnej strony producenta) oferowanego urządzenia.

Kryterium temu zostaje przypisana liczba 15 punktów. Liczba punktów poszczególnym Wykonawcom za kryterium przyznawana będzie według poniższej zasady:

Oferta o najdłuższym czasie bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń otrzyma 15 punktów.

Pozostałe oferty - liczba punktów wyliczona wg wzoru:

*czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń oferty badanej*

*Pi  = ---------------------------------------------------------------------------------------------------------- x 15 pkt*

*najdłuższy czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń spośród nieodrzuconych ofert*

i - numer oferty badanej

Pi - liczba punktów za kryterium „CZAS BEZAWARYJNEJ PRACY (MTBF) DLA ZAPROPONOWANYCH URZĄDZEŃ ” (oferty badanej)

czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń oferty – czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń z Formularza oferty

W przypadku, gdy w ofertach zostanie zaproponowany czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń dłuższy niż 15 lat, do oceny ofert zostanie przyjęte   
15 lat.

Za czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń przyjmuje się liczbę pełnych lat. W przypadku, gdy Wykonawca w Formularzu oferty poda czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń w niepełnych latach np. „11 lat i 5 miesięcy”, przy ocenie oferty Zamawiający zaokrągli czas bezawaryjnej pracy (MTBF) dla zaproponowanych urządzeń w dół do najbliższej pełnej liczby (np. zadeklarowany okres wynoszący „11 lat i 5 miesięcy” zostanie zaokrąglony do 11 lat itp.)

*W imieniu Zamawiającego*

Pełnomocnik Rektora ds. zamówień publicznych

mgr Piotr Skubera