Transportowy Dozór Techniczny
ul. Puławska 125
02-707 Warszawa
tel.: +48 22 490 29 02
e-mail: info@tdt.gov.pl

POLSKA STULECIE ODZYSKANIA NIEPODLEGŁOŚCI

Warszawa, dn. 06.08.2021 r.

Wykonawcy

Nr postępowania ZP 7/2021

Znak sprawy: P.290.3.2021.PZ

dotyczy: postępowania o udzielenie zamówienia publicznego: Dostawa sprzętu sieciowego, Numer referencyjny postępowania: ZP 7/2021

Szanowni Państwo,

uprzejmie informuję, iż do Zamawiającego wpłynęły pytania dotyczące przedmiotowego postępowania. Zamawiający przytacza treść pytań oraz na podstawie art. 135 ust. 2 oraz. art. 137 ust. 1 ustawy Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.), zwaną dalej ustawą Pzp, udziela poniższych wyjaśnień oraz wprowadza zmiany do SWZ.

Pytanie 1:
W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne) w punkcie 1, podpunkcie 13 Zamawiający pisze: Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.

Czy Zamawiający dopuszcza rozpoznawanie plików na bazie innych mechanizmów niż zawartość i metadane? Wielu wiodących producentów NGFW stosuje inne metody identyfikacji plików jak np MIME.

<u>Odpowiedź na pytanie 1</u>
Zamawiający informuje, iż standard MIME określa typ pliku. Bazowanie wyłącznie na identyfikacji MIME ogranicza możliwość rozpoznania zagrożenia. Zamawiający wymaga rozpoznawania plików za pomocą Metadanych, które zawierają szerszą informację niż MIME na temat przesyłanego pliku oraz skanowania zawartości w celu wyeliminowania zagrożenia poprzez sfałszowane informacji w przesyłanych plikach. Funkcjonalności te pozwolą Zamawiającemu w lepszy i bezpieczniejszy sposób monitorować ruch całej sieci.

Pytanie 2
W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne) w punkcie 1, podpunkcie 15 Zamawiający pisze: Urządzenia firewall muszą być wyposażone 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). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 20 użytkowników.

Wybrani producenci firewalli stosują odrębną licencję przy większej ilości użytkowników API. Czy Zamawiający zgadza się na jedno wspólne konto? Czy Zamawiający zatrudnia 20 administratorów systemów firewall, że oczekuje tak dużej ilości kont API?

Odpowiedź na pytanie 2

API – zbiór reguł ściśle opisujący, w jaki sposób programy lub podprogramy komunikują się ze sobą. W związku z powyższym Api jest interfejsem oprogramowania wykorzystywanym przez programistów jak i administratorów oraz programy wykorzystujące ten interfejs. Zatem dostęp do API, dokumentacji i pomocy technicznej producenta musi jednocześnie umożliwiać dostęp dla co najmniej 20 użytkowników wliczając w to programistów, programy jak i administratorów. Zamawiający nie wyraża zgody na wspólne konto z uwagi na brak rozliczalności wykorzystania API przez zewnętrzne systemy. Zgodnie z zapisem „Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji" Zamawiający musi przewidzieć oferowane przez producentów różne rodzaje licencjonowania uwzględniające dostęp urządzeń, oprogramowania czy też użytkowników

Pytanie 3

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne) w punkcie 1, podpunkcie 23 Zamawiający pisze: Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
b. API

Powyższy zapis jest ograniczeniem konkurencji gdyż wprost wskazuje na mechanizmy stosowane przez PaloAltoNetworks. Inni producenci stosują własne, nie mniej skuteczne i przyjazne techniki pozwalające na tworzenie grup użytkowników. Czy Zamawiający dopuszcza inne rozwiązania stosowane przez wiodących producentów systemów firewall do tworzenia grup użytkowników?

Odpowiedź na pytanie 3

Zamawiający nie określił metody tworzenia grup użytkowników a jedynie zgodnie z zapisem wymaga dostarczenia sytemu umożliwiającego tworzenie dynamicznych obiektów, które mogą zostać oznaczona etykietami (tagi). Zapis dotyczący stosowania etykiet (tag) nie jest specyficznym wymogiem, które spełnia wyłącznie tylko jeden producent.

Jednocześnie chcąc uszczegolowić zapis Zamawiajacy zmienia treść SWZ Załacznik nr 1 Opis przedmiotu zamówienia po zmianie 29.07.2021, w III pkt 1 ppkt 23 w następujacy sposób:

Treść
23. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
b. API.

Otrzymuje następujące brzmienie:
23. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
b. API.
lub równoważny
Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników.
Musi istnieć możliwość dynamicznego przypisania użytkownika do grupy w odpowiedzi na wykryte przez firewall zdarzenia bezpieczeństwa powiązane z tym użytkownikiem.
Musi istnieć możliwość zdefiniowania poziomu krytyczności zdarzenia bezpieczeństwa, które wyzwoli automatyczne przypisanie użytkownika do grupy.
Musi istnieć możliwość przypisania użytkownika do takiej grupy również przez zewnętrzne narzędzia bezpieczeństwa celem umożliwienia integracji systemów bezpieczeństwa w obecnym i przyszłym posiadaniu Zamawiającego. Urządzenie musi realizować w/w integrację przez API.
Do dynamicznej grupy użytkowników musi być dodawana nazwa użytkownika. Nie dopuszcza się, aby do takiej grupy dodawany był tylko adres IP.

Pytanie 4

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne) w punkcie 1, podpunkcie 44 Zamawiający pisze:

Urządzenia firewall muszą posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na dobę i pochodzić od tego samego producenta co firewall.

Wymóg odnośnie bazy sygnatur pochodzących od tego samego producenta co firewall jest ograniczeniem konkurencji. Nadmieniamy, że większa ilość źródeł definicji zagrożeń (sygnatur) zwiększa skuteczność detekcji zagrożeń przez urządzenie, atutem więc będzie w tym przypadku możliwość wykorzystywania maksymalnej ilości baz sygnatur a nie tylko jednej bazy pochodzącej od producenta urządzenia. Czy Zamawiający dopuszcza urządzenia korzystające z różnych baz sygnatur?

<u>Odpowiedź na pytanie 4</u>

Zapis „pochodzić od tego samego producenta co firewall" jest wymaganiem minimalnym, a Zamawiający dopuszcza rozwiązanie, które bazuje na sygnaturach innych producentów rozwiązań antywirusowych akceptowanych przez producenta urządzenia oraz jest synchronizowane z serwerów producenta urządzenia.

Pytanie 5

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne) w punkcie 1, podpunkcie 48 Zamawiający pisze: Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox" plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Oczekiwany interwał aktualizacji raz na dobę.

Jaki konkretnie model sandbox (producent i model) posiada Zamawiający? Wiedza nt. oczekiwań Zamawiającego odnośnie integracji z konkretnym systemem sandbox pozwoli nam dobrać właściwe urządzenie.

<u>Odpowiedź na pytanie 5</u>

Zamawiający obecnie nie posiada rozwiązania typu SandBox. Zamawiający w specyfikacji określił funkcjonalność, którą może wykorzystać w przyszłości bez potrzeby określania konkretnego rozwiązania typu Sandbox w formie urządzenia lub w formie usługi chmurowej.

Pytanie 6:

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Wymagania dodatkowe - urządzenia Centralne – 2 szt. (para HA) w punkcie 2, podpunkt 3 Zamawiający pisze: Urządzenie musi być wyposażone w dysk systemowy SSD minimum 220 GB potrzeby systemu operacyjnego i logów. Dysk musi mieć możliwość wymiany bez potrzeb rozkręcania urządzenia.

Czy Zamawiający zgadza się w razie konieczności naprawy firewalla na pozostawienie u Zamawiającego całego urządzenia a nie tylko dysków? W ten sposób Zamawiający osiągnie cel - żadne dane nie opuszczą jego siedziby nawet w sytuacji konieczności wymiany całego urządzenia.
Odnośnie oczekiwanej pojemności dysku i jego rodzaju (SSD). Dlaczego Zamawiający oczekuje konkretnych dysków skoro nie może posiadać wiedzy nt. sposobu zapisu danych stosowanych przez konkretnych producentów. Nadmieniamy, że w przypadku dysków SSD występuje ograniczona ilość zapisów co przekłada się na krótszą żywotność tych dysków oraz znacznie trudniejszy proces odzyskiwania danych w razie ich awarii w porównaniu do dysków magnetycznych. Producenci stosują również różne metody kompresji danych co oznacza, że na wymaganym dysku 220GB (dyski używane przez PaloAltoNetworks) można zapisać historię logów z kilku dni lub kilku miesięcy - w zależności od stopnia kompresji stosowanej przez producenta firewalla. Oczekujemy, że Zamawiający przedstawi

swoje potrzeby biznesowe w postaci oczekiwanej retencji danych lub minimalnej ilości dni przechowywanej historii logów a nie specyfiki dysków używanych przez jednego producenta co stanowi istotne ograniczenie konkurencji.

Odpowiedź na pytanie 6

Pytanie wykonawcy nie odnosi się do zmienionego OPZ, który uwzględnia warunek równoważny.
Zgodnie ze zmienionym zapisem w przypadku wymiany uszkodzonego urządzenia Zamawiający wymaga pozostawienia dysku u Zamawiającego. Jeżeli Wykonawca w ramach naprawy dokona wymiany całego urządzenia bez potrzeby zwrotu urządzenia wraz z dyskiem to Zamawiający uzna warunek „wymiana uszkodzonego urządzenia będzie umożliwiała odesłanie urządzenia (RMA) bez nośnika danych (dysku)" jako spełniony.
Ponadto Zamawiający oczekuje dostawy urządzeń wraz z dyskami SSD. Zamawiający informuje również, iż obecnie minimalna ilość przetwarzanych logów na dzień wynosi około 145GB.

Pytanie 7:

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, Wymagania dodatkowe - urządzenia Centralne – 2 szt. (para HA) w punkcie 2, podpunkt 8 Zamawiający pisze:
Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać zaawansowane funkcjonalności:

a. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)

b. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS, Google Android.

c. Dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-13), Android (6-10), Win 10 UWP

d. Dostępność oprogramowania klienta VPN dla stacji/laptopów z systemami: Windows 7-10, Ubuntu 14-20, CentOS 7-8, macOS 10.11-10.15.

e. Możliwość zestawiania połączeń zdalnego dostępu VPN za pomocą IPv6

f. Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. dla systemów Windows.

g. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows.

h. Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów
Windows i MacOS.

Odnośnie pkt d SIWZ: Prosimy o wskazanie z jakich systemów operacyjnych przy połączeniach VPN korzysta Zamawiający. Prosimy o podanie faktycznych systemów operacyjnych wykorzystywanych w środowisku TDT (analiza historycznych zapytań w przetargowych TDT nie wskazuje na istnienie np. CentOS czy Ubuntu).

Odpowiedź na pytanie 7

Zamawiający zgodnie z wymaganiem dla klienta VPN wymienia wszystkie popularne systemy obecne na rynku, jednocześnie Zamawiający informuje, iż w środowisku TDT są użytkowane systemy klasy Microsoft Windows, Unix i Linux.

Pytanie 8:

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, tabela Centralny system zarządzania – 1 szt. w punkcie 1, podpunkt 5 Zamawiający pisze: System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne:
a. obsługa nie mniej niż 25 firewalli Dostawa sprzętu sieciowego Numer referencyjny postępowania: ZP 7/2021
b. w przyszłości możliwość rozbudowy zarządzania do 500 urządzeń (jeżeli jest wymagana specjalna licencja na ilość urządzeń w chwili dostawy wymagana jest dla punktu a – 25 urządzeń i możliwość rozbudowy w przyszłości).
c. zasób dyskowy RAID1 w rozmiarze 16TB (np. 4 dyski 8TB pracujące w parach niezawodnościowych).
d. zapewnienie możliwości rozbudowy przestrzeni RAID1 do rozmiaru 48 TB za pomocą dokupienia dodatkowych dysków (np. 12 dysków po 8TB) bez potrzeby zakupu dodatkowych licencji lub subskrypcji.

Odnośnie pkt b. Prosimy o potwierdzenie ilość firewalli wykorzystywanych obecnie lub planowanych do zakupu w okresie 3-5 lat (typowy okres eksploatacji dla urządzeń firewall). Zamawiający oczekuje obecnie systemu mającego możliwość rozbudowy do 500 szt firewalli! Informujemy jako profesjonalny dostawca setek firewalli dla rynku dużych klientów, że w Polsce nie istnieje żadna organizacja korzystająca z takiej ilości firewalli.

Odnośnie pkt c i d. Prosimy o wskazanie oczekiwanego okresu przechowywania logów oraz ich retencji. Wymóg rozbudowy do 48TB nie jest wymaganiem funkcjonalnym i nie mówi nic o długości oraz ilość przechowywanych danych z uwagi na różne mechanizmy kompresji stosowane przez różnych producentów. Obecny zapis stanowi ograniczenie konkurencji i wskazuje na producenta PaloAltoNetworks model Panorama M600
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/panorama-centralized-management-datasheet

Odpowiedź na pytanie 8
Pytanie jest skierowane do poprzedniej wersji OPZ.
Zamawiający musi przewidzieć w ramach zamówienia możliwość rozwoju firmy, ponadto zgodnie z przewidywaniami planuje użytkować zamówione urządzenia co najmniej 8-10 lat zatem na taki okres użytkowania Zamawiający planuje dokupienie co najmniej kilkudziesięciu urządzeń w tym okresie oraz wzrost ilości logów generowanych przez te urządzenia. W związku z powyższym Zamawiający dokonuje modyfikacji specyfikacji w tym zakresie.

Zamawiający zmienia treść SWZ Załacznik nr 1 Opis przedmiotu zamówienia po zmianie 29.07.2021, w IV pkt 1 ppkt 5 w następujacy sposób:

Treść
5. System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne:
   a. obsługa nie mniej niż 25 firewalli
   b. w przyszłości możliwość rozbudowy zarządzania do 500 urządzeń (jeżeli jest wymagana specjalna licencja na ilość urządzeń w chwili dostawy wymagana jest dla punktu a – 25 urządzeń i możliwość rozbudowy w przyszłości).
   c. zasób dyskowy RAID1 w rozmiarze 16TB (np. 4 dyski 8TB pracujące w parach niezawodnościowych).
   d. zapewnienie możliwości rozbudowy przestrzeni RAID1 do rozmiaru 48 TB za pomocą dokupienia dodatkowych dysków (np. 12 dysków po 8TB) bez potrzeby zakupu dodatkowych licencji lub subskrypcji.
   e. Wymiana uszkodzonego urządzenia umożliwia odesłanie urządzenia (RMA) bez nośników danych (dysków).

Otrzymuje następujące brzmienie:
5. System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne:
   a. obsługa nie mniej niż 25 firewalli
   b. w przyszłości możliwość rozbudowy zarządzania do 400 urządzeń (jeżeli jest wymagana specjalna licencja na ilość urządzeń w chwili dostawy wymagana jest dla punktu a – 25 urządzeń i możliwość rozbudowy w przyszłości).
   c. zasób dyskowy RAID w rozmiarze co najmniej 16TB.
   d. zapewnienie możliwości rozbudowy przestrzeni RAID do rozmiaru co najmniej 48 TB lub więcej za pomocą dokupienia dodatkowych dysków bez potrzeby zakupu dodatkowych licencji lub subskrypcji.
      Zamawiający dopuszcza dostarczenie systemu, który nie będzie posiadał opcji rozbudowy, ale w momencie dostawy będzie posiadał przestrzeń RAID o rozmiarze co najmniej 48TB.
   e. Wymiana uszkodzonego urządzenia umożliwia odesłanie urządzenia (RMA) bez nośników danych (dysków).

Na podstawie art. art. 137 ust. 2 ustawy Pzp, Zamawiający udostępnia wyjaśnienia SWZ i dokonaną zmianę treści SWZ na stronie internetowej prowadzonego postępowania, na której udostępniona jest SWZ i jest ona wiążąca.

Załączniki:

Załącznik nr 1 Opis przedmiotu zamówienia - po zmianie z dnia 06.08.2021r.