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

Warszawa, dn. 01.06.2021 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 nr 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 2 Zamawiający pisze: Specjalizowane urządzenia sieciowe i towarzyszące oprogramowanie musi być dostarczone i wspierane przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat.

Zapis dotyczący istnienia 5 lat w ćwiartce Gartnera Leaders ogranicza konkurencję, poza poza PaloAlto Networks i CheeckPoint. Okres 5 lat w IT to bardzo długi okres podczas którego pojawiają się nowe generacje urządzeń ale poprzez takie ograniczenie Zamawiający wyklucza nowych i innowacyjnych producentów. Z jakiego powodu wymagany jest okres 5 lat w ćwiartce Leaders w raportach Gartner Magic Quadrant for Enterprise Network Firewalls? Ten zapis wyklucza lidera runku rozwiązań firewall - firmę Fortinet, która oferuje szerszą niż PaloAlto gamę funkcjonalności a jej rozwiązania są istotnie korzystniejsze cenowo od PaloAlto. Rozumiejąc obawy Zamawiającego o pojawienie się ofert z egzotycznymi producentami rekomendujemy skrócenie okresu przebywania firmy w ćwiartce liderów do 3 lat (Fortigate - jest ćwiartce liderów od 4 lat).

Odpowiedź na pytanie 1

Zamawiający nie zmienia treści SWZ w powyższym zakresie.

Pytanie nr 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 4 Zamawiający pisze: Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden port konsoli USB Micro-B, oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T.

Specyficzny port USB Micro-B jest wymogiem ograniczającym konkurencję - wielu wiodących producentów opiera się na tradycyjnym porcie konsolowym oraz porcie zarządzającym co jest praktyką rynkową - nie ma żadnego uzasadnienia merytorycznego do tego wymogu. W przypadku wiodących producentów NGFW tylko jeden producent spełnia ten

wymóg (Palo Alto Networks). Dlaczego Zamawiający wymaga portu USB Micro-B a nie np. innego, bardziej popularnego standardu np RJ45, który umożliwia realizację tych samych funkcji?

Odpowiedź na pytanie 2:

Zamawiający zmienia treść SWZ - Załacznik nr 1 Opis przedmiotu zamówienia pkt III.1.4 w następujący sposób:

Aktualny zapis:

„Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden port konsoli USB Micro-B, oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T."

Otrzymuje następujące brzmienie:

Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 lub w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T. Wymagane jest dostarczenie wraz z oferowanymi urządzeniami odpowiednich kabli konsolowych, które umożliwiają podłączenie ich do komputera przez port USB 2.0 lub 3.0.

Pytanie nr 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 5 Zamawiający pisze: Urządzenia firewall muszą posiadać budowę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (tzw. Data Plane).

Wielu wiodących producentów urządzeń FW opiera separację na oddzielnych systemach wirtualnych a nie procesorach. Ten wymóg wyklucza wielu wiodących producentów firewalli. Dlaczego klient wymaga takiej budowy firewalli skoro nie ma ona wpływu na funkcjonalność i wydajność urządzeń?

Odpowiedź na pytanie 3:

Wymóg jest podyktowany potrzebami Zamawiającego, w tym zakresie (szczególny przypadek bezpieczeństwa ochrona przez atakami typu DoS, DDoS) z uwagi na separację sprzętową a nie programową. W przypadku zastosowania rozwiązania programowego istnieje możliwość zablokowania całego urządzenia poprzez wykorzystanie całej mocy procesora, która uniemożliwi w przypadku skutecznego ataku zarządzanie urządzeniem, zatem błędnym jest twierdzenie, iż nie ma to wpływu na funkcjonalność i wydajność urządzenia. Zamawiający jak i wykonawca nie ma możliwości przewidzenia w jakim zakresie nastąpi atak typu DoS, DDoS, który może doprowadzić do zablokowania urządzenia co będzie miało przełożenie na zastosowanie odpowiednia wydajnego procesora. Zatem jak należy zauważyć zamawiający w ramach wymagania określił, iż preferuje rozwiązanie, które nie spowoduje zablokowania urządzenia w całości, a jedynie zablokuje część odpowiedzialną za ruch sieciowy, dając jednocześnie zamawiającemu możliwość kontroli nad urządzeniem. Ponadto na rynku urządzeń typu firewall są dostępne rozwiązania z separacją ruchu Management Plane i Data Plane.

Przyładowe opis zastosowanego rozwiązania firmy Checkpoint:

https://community.checkpoint.com/t5/Security-Gateways/New-R80-30-feature-Management-Data-Plane-Separation-for-gateways/td-p/47633 ,

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk138672.

Przyładowe opis zastosowanego rozwiązania firmy PaloAlto Networks:

https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures

Pytanie nr 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 6 Zamawiający pisze: Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.

Zapis faworyzujący producenta o konkretnej architekturze (PaloAltoNetworks) bez uzasadnienia merytorycznego - w konkurencyjnych do PaloAlto firewallach nadmierne obciążenie data plane jest niwelowane przez zastosowanie odpowiednio wydajnego urządzenia. Prosimy o przedstawienie statystyk ruchu które pozwolą nam dobrać urządzenia

wykluczające ich nadmierne obciążenie zamiast obecnie podawanych parametrów wydajnościowych firewall konkretnego producenta (Palo Alto Networks).

Odpowiedź na pytanie 4

W odpowiedzi należy uznać, iż powyższy zapis nie faworyzuje żadnego producenta z uwagi na to, że zamawiający sformułował ten punkt, który dotyczy większości urządzeń sieciowych czy to z separacją sprzętową, czy też z separacją programową (wirtualną), że w przypadku znacznego obciążenia ruchem części odpowiedzialnej za obsługę ruchu sieciowego nie powinno to wpływać na część urządzenia odpowiedzialną za zarządzanie i monitorowanie urządzenia czy to przez zastosowanie separacji sprzętowe,j czy też zastosowanie wydajnego urządenia „Wielu wiodących producentów urządzeń FW opiera separację na oddzielnych systemach wirtualnych a nie procesorach". W związku z żądaniem przedstawienia statystyk ruchu sieciowego zamawiający informuje, iż przedstawił w opisie przedmiotu zamówienia minimalne wymagania dotyczące wydajności urządzeń sieciowych, które będą używane w perspektywie co najmniej 8 do 10 lat (Zamawiający obecnie użytkuje urządzenia nabyte w 2014 r.), zatem Zamawiający musiał przewidzieć konieczność zwiększenia wymagań dla urządzeń z uwagi na planowany rozwój firmy. Reasumując ten punkt nie może być podstawą do żądań wykonawcy o zmianę tego wymagania, ponieważ wykonawca może zaoferować urządzenie które będzie spełniało minimalne wymagania Zamawiającego co do wydajności urządzenia a nadmierne obciążenie data plane będzie niwelowane przez zastosowanie odpowiednio wydajnego urządzenia. Ponadto z uwagi na brak personelu odpowiedzialnego za zarządzanie urządzeniami IT w jednostkach terenowych TDT powyższy zapis jest podyktowany potrzebami zamawiającego z uwagi na konieczność zdalnego zarządzania urządzeniami a stabilna praca urządzenia jest dla Zamawiającego najważniejsza.

Pytanie nr 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 7 Zamawiający pisze:

Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.

Ile VLANów obecnie posiada TDT? Wymóg jest według nas przewymiarowany. Analiza historycznych zapytań TDT w trybie PZP wskazuje na ok 300 użytkowników w sieci TDT - skąd zatem wymóg posiadania 4 tys VLAN (sieci wirtualnych) dla urządzeń firewall i to w każdej lokalizacji?

Odpowiedź na pytanie 5:

Zastosowana u Zamawiającego polityka „zero-trust" wymaga podziału na wiele segmentów sieci uwzględniających aspekty zarządzania budynkami (monitoring, systemy bezpieczeństwa, itp.), uwzględniającymi również strukturę organizacyjną zamawiającego. Aktualnie zamawiający posiada skonfigurowanych kilkadziesiąt intererfejsów VLAN. Jednocześnie Zamawiający pragnie zakwestionować twierdzenia pytającego o wymaganiach konfiguracji na urządzeniach 4000 interfejsów VLAN z uwagi na błędne zinterpretowanie tego zapisu, mówi wyłącznie o możliwości wprowadzenia w urządzeniu 4000 identyfikatorów/znaczników, a nie mówi o konieczności tworzenia 4000 subinterfejsów L3 lub 4000 vlanów. Zgodnie z powyższym można stwierdzić, iż w wyniku błędnej interpretacji tego punktu przez pytającego Zamawiający nie spowodował ograniczenia konkuręcji, w tym zakresie co znajduje odzwierciedlenie w informacji zawartej w poniższym linku dotyczącej oprogramowania na urządzenia firewall producenta Fortinet „Identyfikator sieci VLAN to liczba z zakresu od 1 do 4094, która umożliwia łączenie grup adresów IP o tym samym identyfikatorze sieci VLAN.

https://docs.fortinet.com/document/fortigate/6.0.0/handbook/153929/vlans

Pytanie nr 6:

Zamawiający wymaga aby urządzenia obsługiwały min 4000 VLAN - prosimy o informację ilu pracowników zatrudnia Zamawiający, że wymaga aby urządzenia zapewniały obsługę 4000 znaczników VLAN (odrębnych segmentów sieci).

Odpowiedź na pytanie 6:

Obecnie Zamawiający zatrudnia około 380 osób, jednak planowane jest zwiększenie zatrudnienia zgodnie z treścią odpowiedzi na pytanie nr 5.

Pytanie nr 7:

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 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).

Prosimy o szczegółowe informacje z jakimi produktami, producentami Zamawiający zamierza się integrować za pomocą API aby Oferent mógł dobrać rozwiązanie.

Odpowiedź na pytanie 7:

Intencją Zamawiającego jest posiadanie możliwości orkiestracji firewalli przez inne systemy w przyszłym posiadaniu Zamawiającego celem zwiększenia bezpieczeństwa systemów, poprzez uzyskanie możliwości integracji różnych systemów bezpieczeństwa.

Zamawiający ma wiedzę, że najpopularniejszą formą takiej integracji jest interfejs programistyczny API udostępniony w formie tzw. web-service'u.

Zamawiający dopuszcza dowolną formę kodownia danych oraz wywołań API, tak długo dopóki warstwą transportową pozostaje protokół HTTPS, dane są kodowane z wykorzystaniem XML lub JSON, a dokumentacja API jest publicznie dostępna na stronach producenta.

Pytanie nr 8:

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 19 Zamawiający pisze: Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.

Prosimy o informację o wykorzystywanych w TDT stanowiskach terminalowych, które mają być objęte polityką kontroli dostępu

Odpowiedź na pytanie 8:

Zamawiający wykorzystuje środowisko terminalowe systemu Windows Server.

Pytanie nr 9:

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 20 Zamawiający pisze:

Urządzenia firewall muszą umożliwiać synchronizację i wymianę danych o użytkownikach pomiędzy sobą z wykorzystaniem centralnego systemu zarządzania opisanego w dalszej części wymagań.

Jakiego rodzaju dane, w jakim formacie i trybie synchronizacji ma się to odbywać?

Odpowiedź na pytanie 9:

Zamawiający wymaga synchronizacji urządzeń z usługą katalogową active directory lub usługą LDAP, zgodnie z tym protokołem w celu weryfikacji użytkowników, jednocześnie nie narzuca wykonawcy sposobu komunikacji i synchronizacji urządzeń firewall z systemem centralnego zarządzania.

Pytanie nr 10:

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 22 Zamawiający pisze: Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.

Skoro Zamawiający oczekuje centralnego systemu zarządzania i raportowania dla wszystkich NGFW to dlaczego wymaga aby raportowanie odbywało się bezpośrednio z poziomu pojedynczych urządzeń? Jest to ograniczenie konkurencji ponieważ różni producenci oferują różne techniczne ale funkcjonalnie tożsame rozwiązania w tym zakresie.

Odpowiedź na pytanie 10:

Celem jest zapewnienie możliwości nieprzerwanej kontroli poziomu bezpieczeństwa infrastruktury Zamawiającego i analizy incydentów bezpieczeństwa nawet w przypadku braku komunikacji między urządzeniem Firewall a centralnym systemem zarządzania. Należy wziąć pod uwagę, że infrastruktura jest rozproszona geograficznie, a jej poszczególne węzły łączą się z jej punktem centralnym poprzez sieć niezależnego dostawcy (dostawców). Konieczne jest ograniczenie ryzyka znacznej utraty funkcji bezpieczeństwa w czasie awarii po stronie dostawcy łączy. Rozwiązanie, w którym pomimo braku połączenia do centralnego systemu zarządzania, administratorzy mają możliwość analizy logów i tworzenia raportów bezpośrednio na urządzeniach Firewall jest najbardziej optymalne i efektywne kosztowo (w szczególności nie wnosi kosztów utrzymania dodatkowych systemów przetwarzania logów i raportowania w poszczególnych lokalizacjach).

Zamawiajacy zmienia treść SWZ Załacznik nr 1 Opis przedmiotu zamówienia pkt III.1.22.

Treść zapisu:

„Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu."

otrzymuje następujące brzmienie:

Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF i CSV. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Sposób realizacji możliwy jest również jako rozwiązanie równoważne przez dostarczenie dodatkowego, lokalnego systemu logowania który powinien mieć takie same możliwości w każdej lokalizacji objętej postępowaniem. Po odzyskaniu połączenia z punktem centralnym musi być możliwe zsynchronizowanie lokalnych logów i raportów z lokalnych systemów z centralnym systemem zarządzania. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji, musi zostać zapewniony poziom redundancji zasilania i dysków, który umożliwi kontynuację pracy nawet w wypadku awarii jednego z tych komponentów.

W odpowiedzi na pytanie *„Skoro Zamawiający oczekuje centralnego systemu zarządzania i raportowania dla wszystkich NGFW to dlaczego wymaga, aby raportowanie odbywało się bezpośrednio z poziomu pojedynczych urządzeń?*" Zamawiający pragnie wyjaśnić, iż zgodnie z ROZPORZĄDZENIEM RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i zgodnie z § 20 ust 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zatem zamawiający musi przewidzieć, w tym zakresie awarie komunikacji z systemem centralnego zarządzania lub jego awarią i mieć dalszą możliwość możliwość utrzymywania zgodności z tym artykułem.

Pytanie nr 11:

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 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

Czym podyktowana jest funkcjonalność bazowania na etykietach? Czy Zamawiający może podać przykład wykorzystania tej funkcjonalności? W jaki sposób Zamawiający zamierza wykorzystać interface API przy wykorzystaniu

grup bazujących na etykietach? Czy jedynym oczekiwaniem efektem tej funkcjonalności jest bazowania na tagach zamiast na grupach użytkowników? Ten sam efekt producenci firewalli osiągają w standardowy sposób bazując na grupach użytkowników - tagi nie wnoszą żadnej wartości funkcjonalnej. Zapis dot tagi jest specyficznym wymogiem spełnianym wg naszej wiedzy przez jednego producenta.

Odpowiedź na pytanie 11:

Intencją Zamawiającego jest posiadanie możliwości korzystania z etykiet z uwagi na zarządzanie dużą liczbą polityk bezpieczeństwa a które pozwalają na sprawne zarządzanie tymi politykami.

Zamawiający wykorzystuje obecnie opisaną funkcjonalność w swoich systemach, które są obecnie w posiadaniu przez Zamawiającego.

Zamawiający informuje, iż metody wykorzystania interfejsu API określa producent a dokumentacja powinna być dostępna na stronach producenta.

Pytanie nr 12:

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 25 Zamawiający pisze:

Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF dla IPv4 i IPv6.

Czy Zamawiający używa któregokolwiek z wymaganych protokołów routingu? Jeśli wymogiem Zamawiającego jest przełączanie funkcji bezpieczeństwa w przypadku awarii łącza to tożsamym funkcjonalnie jest opcja PBF „policy base forwarding" Czy Zamawiający dopuszcza zastosowanie tożsamej funkcji PBF zamiast BGP i OSPF?

Odpowiedź na pytanie 12:

Aktualnie Zamawiający nie wykorzystuje protokołów routingu dynamicznego jednocześnie intencją Zamawiającego jest posiadanie możliwości obsługi protokołu BGP z uwagi na możliwe użycie tego protokołu w sieci wewnętrznej zamawiającego. Jednocześnie Zamawiający również wykorzystuje obecnie opcję PBF.

Pytanie nr 13:

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 27 Zamawiający pisze:

Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

Z jakiego powodu firewalle muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa skoro oba te obszary są ściśle związane ze sobą i wielu producentów konfigurowane w jednym oknie GUI? Jest to nieuzasadnione ograniczenie konkurencji gdyż nie dotyczy funkcjonalności ale raczej wyglądu interfejsu użytkownika.

Odpowiedź na pytanie 13:

Ustawienia NAT konfiguruje się sporadycznie. Natomiast Polityki bezpieczeństwa zmienia się częściej. Przy oddzieleniu Polityk bezpieczeństwa od NAT jest możliwość zmiany działania bardziej globalnie.

Kilku producentów Firewall oferuje rozwiązania spełniające wymaganie rozdzielenia reguł NAT od polityk bezpieczeństwa.

Z doświadczenia zamawiającego translację adresów NAT ustawia się sporadycznie, zaś polityki bęzpiecznstwa są modyfikowane bardzo często zatem takie zdefiniowanie interfejsu najbardziej odpowiada Zamawiającemu z uwagi na rozdzielenie tych polityk co znacznie wpływa na przejżystość rozwiązania. W związku z powyższym interfejs użytkownika jest również funkcjonalnością urządzenia i niejednokrotnie umożliwia interakcję z urządzeniem. Ponadto na rynku producentów urządzeń Firewall oferuje się rozwiązania spełniające wymaganie rozdzielenia reguł NAT od polityk bezpieczeństwa.

W przypadku producenta CheckPoint:

https://www.youtube.com/watch?v=PvcQmN2QAvs

https://www.youtube.com/watch?v=6ZbkOXoihak

Pytanie nr 14:

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 na potrzeby systemu operacyjnego i logów. Dysk musi mieć możliwość wymiany bez potrzeb rozkręcania urządzenia.

Z jakiego powodu Zamawiający wymaga, aby urządzenie było wyposażone w dysk systemowy SSD minimum 220 GB potrzeby systemu operacyjnego i logów oraz dysk musi mieć możliwość wymiany bez potrzeb rozkręcania urządzenia? Zapis ten wyklucza konkurencyjne rozwiązania poza Palo Alto Networks. Procedura wymiany dysków w praktyce nie występuje podczas eksploatacji systemu a w sytuacji awarii firewalla wymianie podlega całe urządzenie. Dlaczego Zamawiający wymaga konkretnie dysków SSD wewnątrz firewalla skoro producenci firewalli stosują różne rozwiązania pamięci masowej uzyskując ta samą funkcjonalność? Dlaczego Zamawiający wyspecyfikował takie wymagania mając na uwadze, że zamawia również system centralnego zarządzania gdzie będą składowane logi ze wszystkich firewalli?

Odpowiedź na pytanie 14:

Zamawiający wymaga wyposażenia urządzenia w wyjmowane dyski systemowe z uwagi na uzasadnioną potrzebę zamawiającego.

Potrzeba ta podyktowana jest względami praktycznymi z uwagi na umieszczanie urządzeń w szafach wraz z innymi urządzeniami serwerowymi czy też sieciowymi co wiąże się z demontażem urządzeń, okablowania sieciowego jak i zasilania a w przypadku awarii dysku nie jest wymagana wymiana całego urządzenia tylko wymiana dysku bez potrzeby wyjmowania całego urządzenia. Błędnie skarżący założył iż „Procedura wymiany dysków w praktyce nie występuje podczas eksploatacji systemu a w sytuacji awarii firewalla wymianie podlega całe urządzenie" z uwagi na to iż dyski czy to tależowe czy też dyski SSD są urządzeniami elektronicznymi i zawsze mogą ulec uszkodzeniom podczas normalnej eksploatacji. Ponadto wielokrotnie producenci stosują rozwiązania zabezpieczające przed otwieraniem urządzenia w celu wymiany dysku.

Ponadto Zamawiający w przypadku wymagań co do wielkości wielkości dysku w jakie ma być wyposażone urządzenie określił jako wymaganie minimalne z uwagi na konieczność przechowywania znacznej logów stsemowych w długim okresie czasu z uwagi na wymagania wynikające z przepisów ROZPORZĄDZENIEM RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i zgodnie z § 20 ust 4. „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata"

Ponadto na rynku producentów urządzeń Firewall oferuje się rozwiązania spełniające wymagania, które umożliwiają wymianę dysków bez konieczności rozkręcania urządzenia.

W przypadku producenta Checkpoint

https://www.checkpoint.com/downloads/products/7000-security-gateway-datasheet.pdf

Pytanie nr 15:

Zamawiający wymaga możliwości wymiany dysku firewalla bez konieczności rozkręcania obudowy. Taki zapis wyklucza konkurencyjne rozwiązania do Pało Alto Networks, które stosuje nietypowe, niezabezpieczone przed przypadkowym wyciągnięciem dyski. Topowi producenci firewalli zabezpieczają swoje dyski przed możliwością ich przypadkowego wyciągnięcia, abstrahując od faktu, że wyciąganie dysku z urządzeń nie jest podyktowane żadnymi względami praktycznymi a nawet może być powodem do utraty gwarancji. W przypadku wystąpienia awarii producenci w ramach procedur naprawczych wymieniają całe urządzenie na nowe.

Odpowiedź na pytanie 15:

Zgodnie z odpowiedzią na pytanie 14.

Pytanie nr 16:

W SIWZ, w załączniku numer 1 do SIWZ – opis przedmiotu zamówienia, w III. Wymagania dotyczące urządzeń, Wymagania dodatkowe - urządzenia Średnie – 7 szt.

w punkcie 3, podpunkt 2 Zamawiający pisze:

Urządzenie musi być wyposażone w dysk systemowy SSD wielkości minimum 220 GB na potrzeby systemu operacyjnego i logów.

Czym podyktowane jest zastosowanie dysku SSD o tej konkretnej pojemności skoro pojemność dysku nie ma żadnego związku z ilością i okresie przechowywanych danych? Oczekujemy wskazania okresu czasu wymaganego dla retencji danych. Obecny zapis wprost ogranicza konkurencję poza Palo Alto Networks.

Odpowiedź na pytanie 16:

Zgodnie z odpowiedzią na pytanie 14.

Ponadto Zamawiający nie może zgodzić się z twierdzeniem „pojemność dysku nie ma żadnego związku z ilością i okresie przechowywanych danych?" ponieważ zgodnie z informacjami zawartymi odpowiedzi na pytanie nr 14 okres przechowywania danych może wynosić 2 lata zatem Zamawiający określając wymagania minimalne dla zastosowanego dysku ma świadomość, iż taka wielkość może być niewystarczająca.

Pytanie nr 17:

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.

Z czego wynika wymóg odnośnie MacOS? Po prześledzeniu wcześniejszych zapytań Zamawiającego nie znaleźliśmy informacji, żeby Zamawiający występował wcześniej z zapytaniem odnośnie stacji/laptopów z systemem macOS. Czy ewentualnie w TDT istnieją regulacje zezwalające pracownikom na używanie prywatnych urządzeń dowolnego typu i producenta do łączenia się z siecią korporacyjną TDT? Czy Zamawiający wykorzystuje niezwykle rzadko występujące w praktyce IPv6 w swoim środowisku?

Odpowiedź na pytanie 17:

Zamawiający zgodnie z wymaganiem dla klienta VPN wymienia wszystkie popularne systemy obecne na rynku jednocześnie zamawiający nie wyklucza dostępu dla platformy MacOS

Co najmniej kilku producentów urządzeń Firewall oferuje dostępność oprogramowania klienta VPN w wersjach na na urządzenia mobilne jak i systemy komputerowe.

Zamawiający jednocześnie informuję, iż protokół ipv6 jest wykorzystywany poprzez systemy komputerowe zamawiającego.

Pytanie nr 18:

W SIWZ, ROZDZIAŁ 7 Informacja o warunkach udziału w postępowaniu w punkcie 1, podpunkt 2b Zamawiający pisze:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

2) spełniają warunki dotyczące zdolności technicznej i zawodowej:

b) wykaże, iż będzie dysponował przez cały okres realizacji zamówienia zespołem co najmniej trzech osób umożliwiającym realizację zamówienia na odpowiednim poziomie technicznym i wdrożeniowym tj. - osobą pełniącą funkcję kierownika projektu posiadająca certyfikat Prince2 Practicioner oraz ITIL. - osobą pełniącą funkcją konsultanta posiadająca certyfikat inżyniera systemowego wydany przez producenta urządzeń dostarczonych w ramach zamówienia,

- osobą pełniącą funkcję konsultanta posiadająca certyfikat audytora wewnętrznego według normy ISO 22301,

- osobą pełniącą funkcję konsultanta posiadająca certyfikat CIHE,

Jaki jest powód posiadania certyfikatu CIHE? Według nas wymaganie jest nieadekwatne do zapytania ponieważ CIHE Certified Incident Handling Engineer jest specjalistyczną certyfikacją techniczną z zakresu właściwej obsługi incydentów. Obsługa incydentów czyli analiza wyników pracy Firewalla nie jest przedmiotem tego postępowania. Zamawiający nigdzie nie wymaga wsparcia w zakresie obsługi incydentów. Jedynym wymaganiem Zamawiającego jest wykonanie dostawy, wdrożenia oraz świadczenie wsparcia technicznego rozumianego jako wg OPZ.

Odpowiedź na pytanie 18:

Zamawiający zgodnie z uzasadnionymi potrzebami wymaga wsparcia technicznego w zakresie, który wynika z wymagań ROZPORZĄDZENIA RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i zgodnie z § 20 ust. 7 „zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

Zamawiajacy zmienia treść SWZ Załacznik nr 1 Opis przedmiotu zamówienia punkt VII ppkt 4. w nastepujacy sposób:

Treść:

„Wsparcie techniczne będzie polegać w szczególności na:

1) *wsparciu w instalacji oprogramowania, tj. poprawek oprogramowania, najnowszych komercyjnie dostępnych wersji oprogramowania,*
2) *zapewnieniu dostępu do narzędzi konfiguracyjnych i dokumentacji technicznej oprogramowania i urządzeń (o ile nie zapewnia tego producent).”*

Otrzymuje następujące brzmienie:

Wsparcie techniczne będzie polegać w szczególności na:

1) wsparciu w instalacji oprogramowania, tj. poprawek oprogramowania, najnowszych komercyjnie dostępnych wersji oprogramowania,
2) zapewnieniu dostępu do narzędzi konfiguracyjnych i dokumentacji technicznej oprogramowania i urządzeń (o ile nie zapewnia tego producent),
3) obsługa incydentów bezpieczeństwa.

Pytanie nr 19:

Zamawiający wymaga od Wykonawcy certyfikatu CIHE związanego z obsługą incydentów: https://certyfikatit.pl/modules/cihe-certified-incident-handling-engineer/?course_id=1742 co nie jest przedmiotem tego postępowania. Prosimy o usunięcie tego wymagania lub zastąpienie go adekwatnym do przedmiotu zamówienia - np. posiadaniem min 3 inżynierów certyfikowanych w oferowanej technologii co zagwarantuje Zamawiającemu wysoką jakość prac wdrożeniowych.

Odpowiedź na pytanie 19:

Zgodnie z odpowiedzią na pytanie 18.

Pytanie nr 20:

Zamawiający w OPZ podaje wymagane minimalne parametry firewalli o konkretnych wartościach specyficznych dla jednego producenta - Pało Alto Networks. Aby rzetelnie dobrać wydajność urządzeń prosimy o informacje o obecnie obsługiwanym przez firewalle ruchu sieciowym wyrażonym w mbps oraz informację o ewentualnych planowanych procentowych wzrostach ruchu sieciowego w okresie na jaki są kupowane firewalle (w ciagu 3 lat). Bazowanie na granicznych wartościach wydajnościowych konkretnego producenta z kart katalogowych produktów nie umożliwia rzetelnego zaproponowania adekwatnego urządzenia ponieważ każdy producent inaczej podchodzi do liczenia wydajności swoich firewalli. Jedyną możliwością aby oszacować niezbędną wydajność urządzenia jest informacja o konkretnym ruchu sieciowym, który ma zostać podany ochronie.

Odpowiedź na pytanie 20:

Zamawiający uwzględił ruch w swojej sieci i jednocześnie przewidział możliwość jego wzrostu w przypadku rozwoju firmy i uwzględił to w OPZ jako wymagania minimalne.

Skoro wykonawca uważa: „każdy producent inaczej podchodzi do liczenia wydajności swoich firewalli."dlatego też zamawiający nie widzi potrzeby podawania informacji o ruchu sieciowym wyrażonym w mbps z uwagi na brak możliwości porównania tego ruchu.

Zamawiający określił wymagania minimalne do obsługi ruchu sieciowego i oczekuje dostarczenia urządzeń o wydajnościach określonych w OPZ lub wyższych.

Pytanie nr 21:

Ilości interfejsów urządzeń pochodzą wprost z kart katalogowych producenta Palo Alto Networks - proszę o informację ile faktycznie wykorzystują Państwo interfejsów w poszczególnych lokalizacjach.

Odpowiedź na pytanie 21:

Minimalna ilość interfejsów użytych we wszystkich lokalizacjach Zamawiającego waha się pomiędzy 4 a 8 sztukami

Pytanie nr 22:

Zamawiający wymaga aby urządzenia firewall posiadały osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa - w przypadku wiodących producentów firewalli reguły NAT i polityki bezpieczeństwa jako elementy powiązane konfiguruje się w tym samym oknie - wymaganie Zamawiającego należy uznać za nieracjonalne z funkcjonalnego punktu widzenia i skierowane na wyeliminowanie producentów urządzeń bezpieczeństwa poza Palo Alto Networks.

Odpowiedź na pytanie 22:

Zgodnie z odpowiedzią na pytanie 13.

Pytanie nr 23:

Zamawiający w każdym z wymaganych grup urządzeń posługuje się danymi z kart katalogowych Pało Alto Networks formułując swoje wymagania np. dla urządzeń małych 6 szt:
a. Minimum 540 Mbps dla rozpoznawania i kontroli aplikacji,
b. Minimum 320 Mbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
c. Minimum 4 000 nowych sesji na sekundę.
d. Minimum 60 000 równoległych sesji

Proszę o informację jaka jest faktyczna wielkość ruchu sieciowego która ma być poddana ochronie oraz ile faktycznie użytkowników ma obsługiwać ww firewall w lokalizacji, do której planują Państwo tak de facto duże urządzenie. Wg analizy kart katalogowych Palo Alto Networks - ww parametry spełnia model PA220 gdzie wydajność 540 Mbps pozwala jak wynika z naszych doświadczeń na obsługę nawet 100 użytkowników.

Palo Alto Networks ML-Powered Next-Generation Firewall Specifications and Features Summary 2

Table 1: Firewall Performance and Capacities (continued)

Performance and Capacities	PA-850	PA-820	PA-220	PA-220R
Firewall throughput (App-ID, appmix)	2.1 Gbps	1.6 Gbps	540 Mbps	540 Mbps
Threat Prevention throughput (appmix)	1.2 Gbps	900 Mbps	320 Mbps	320 Mbps
IPsec VPN throughput	1.6 Gbps	1.3 Gbps	540 Mbps	540 Mbps
New sessions per second	13,000	8,600	4,300	4,300
Maximum sessions	192,000	128,000	64,000	64,000
Virtual systems (base)	1	1	1	1
Hardware Specifications	**PA-850**	**PA-820**	**PA-220**	**PA-220R**
Interfaces supported[4]	10/100/1000 (4), SFP (4), 10 SFP+ (4)	10/100/1000 (4), SFP (8)	10/100/1000 (8)	10/100/1000 (6), SFP (2)
Management I/O	10/100/1000 out-of-band management (1), 10/100/1000 high availability (2), RJ-45 console (1), USB (1), Micro USB console (1)		10/100/1000 out-of-band management (1), RJ-45 console (1), USB (1), Micro USB console (1)	10/100/1000 out-of-band management (1), RJ-45 console (1), USB (1), Micro USB console (1)
Size	1U, 19" standard rack (1.75" H x 14.5" D x 17.125" W)	1U, 19" standard rack (1.75" H x 14" D x 17.125" W)	1.62" H x 6.29" D x 8.07" W	2.0" H x 8.66" D x 9.25" W
Power supply	450 W AC (2; one is redundant)	200 W	Dual redundant 40 W	None
Redundant power supply	Yes	No	Yes (optional)	None
Disk drives	240 GB SSD		32 GB EMMC	32 GB EMMC
Hot-swappable fans	No		No	No

<u>Odpowiedź na pytanie 23:</u>

Zamawiający uwzględił ruch w swojej sieci i jednocześnie przewidział możliwość jego wzrostu, ponieważ przewiduje rozwój firmy i uwzględił to w OPZ jako wymagania minimalne.

Zamawiający określił wymagania minimalne do obsługi ruchu sieciowego i oczekuje dostarczenia urządzeń o wydajnościach określonych w OPZ lub wyższych.

Jednocześnie umieszczamy link do produktu firmy Checkpoint, który spełnia minimalne wymagania OPZ

<u>https://www.checkpoint.com/downloads/products/1500-security-gateway-datasheet.pdf</u>

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 01.06.2021r.