Urząd Lotnictwa Cywilnego
Dyrektor Generalny
Hanna Mazurkiewicz
ul. M. Flisa 2, 02-247 Warszawa
Tel.: + 48 22 520-74-16, Fax: + 48 22 520-73-05

ULC-BDG-GW-260-01/01/20

Warszawa, dnia 07.07.2020 roku

Wykonawcy biorący udział w postępowaniu

dotyczy: *postępowania nr ULC-BDG-GW-260-01/2020 o udzielenie zamówienia publicznego na dostawę, konfigurację i uruchomienie infrastruktury informatycznej wraz ze szkoleniami*

Urząd Lotnictwa Cywilnego występując jako Zamawiający w postępowaniu o udzielenie zamówienia publicznego, prowadzonego w trybie przetargu nieograniczonego, na dostawę, konfigurację i uruchomienie infrastruktury informatycznej wraz ze szkoleniami, działając zgodnie z art. 38 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843), zwanej dalej „ustawą Pzp", w związku z wnioskami o wyjaśnienie treści specyfikacji istotnych warunków zamówienia, które wpłynęły do zamawiającego w dniach 25 czerwca – 6 lipca 2020 roku, udziela następujących wyjaśnień w formie odpowiedzi na pytania Wykonawców:

Pytanie nr 1:

Czy Zamawiający dopuszcza rozwiązanie typu "Zapora sieciowa NGFW", które nie wspiera następujących punktów:

1. 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 lub będzie dostępna przy próbie otwarcia stron blokowanych przez profil ochronny wykorzystujący kategoryzację producenta I interakcję z Sandbox.

2. System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub

stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

3. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci - integracja z Citrix.

4. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".

5. Wsparcie dla protokołów Kerberos, SAML 2.0.

6. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.

Odpowiedź Zamawiającego:

Zamawiający nie zgadza się na rezygnację ze wsparcia funkcjonalności opisanych w punktach 1-6, podtrzymując dotyczasowe zapisy SIWZ.

Pytanie nr 2:

Pytanie dotyczy pkt "Zapora sieciowa – oddziałowa" Czy Zamawiający dopuści rozwiązanie typu "Zapora sieciowa – oddziałowa" posiadające 512MB pamięci flash zamiast opisywanych 4GB?

Odpowiedź Zamawiającego:

Nie, Zamawiający wymaga urządzenia o parametrach zgodnych z SIWZ.

Pytanie nr 3:

Zamawiający w podrozdziale 8.11 "System Backupu" w tabeli 18 "Minimalne wymagania dla urządzenia do składowania danych oraz deduplikacji" oczekuje w punktach: 17. "Oferowany produkt musi umożliwiać replikację danych realizowaną między urządzeniami. Replikacja powinna umożliwiać szyfrowanie przesyłanych danych - długość klucza

minimum 256-bit. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność." W punkcie 18: "Urządzenie musi umożliwiać replikację danych z mniejszymi i większymi modelami urządzeń tego samego producenta. Urządzenie musi umożliwiać replikację danych z edycjami wirtualnymi." oraz w punkcie 19 "Replikacja musi być możliwa w trybie co najmniej 10 do 1 (many to one) oraz co najmniej 1 do 2 (fan out). Kaskadowanie replikacji jest opcjonalne.". Jednocześnie Zamawiający oczekuje dostawy tylko 1 urządzenia. Czy Zamawiający w obecnej chwili posiada już rozwiązanie, które będzie wykorzystane do replikacji wraz z oferowanym rozwiązaniem? Jeśli tak, to czy Zamawiający może udzielić informacji o nazwie i modelu rozwiązania już posiadanego?

Odpowiedź Zamawiającego:

Zamawiający w punktach 17 - 19 określił funkcjonalności urządzenia, które będzie pełniło rolę deduplikatora dla oprogramowania backupu wyspecyfikowane w Tabeli 17. Wykonawca powinien dostarczyć urządzenie spełniające parametry określone w SOPZ przez Zamawiającego.

Pytanie nr 4:

Pytania dotyczące SIWZ.

Dotyczy załącznika nr 1A do SIWZ – wykaz dostarczanych produktów. Zamawiający w tabeli 1 zakres rzeczowy wymaga podania „Oferowane urządzenie (producent, model, główny part number, link do specyfikacji produktu lub dostarczenie dokumentacji)". Prosimy o informację co powinna zawierać wymieniana w tabeli specyfikacja produktu (Zamawiający wymaga podania linku lub dostarczenia dokumentacji) – jednocześnie dalsza część wykazu dostarczanych produktów zdaje się zawierać wystarczające potwierdzenie spełniania podanych parametrów. Czy Zamawiający wymaga aby wymienia specyfikacja techniczna zawierała dodatkowe potwierdzenie spełniania stawianych wymagań? Czy dokumentację należy załączyć do oferty czy też uzupełnić na wezwanie Zamawiającego?

Odpowiedź Zamawiającego:

Zamawiający wymaga podania linku do dokumentacji technicznej producenta lub dokumentacji technicznej w celu weryfikacji oferowanego produktu. W przypadku podania linku, link należy podać w załączniku nr 1A do SIWZ a w przypadku dostarczenia dokumentacji należy dostarczyć razem z ofertą.

Pytanie nr 5:

Dotyczy 8.7. Pamięć blokowa – pkt 5. Zdanie „Macierz musi obsługiwać dyski twarde typu SSD oraz być przystosowana." wydaje się nie mieć zakończenia. Czy Zamawiający oczekuje macierzy przystosowanej do obsługi dysków HDD? Prosimy o wyjaśnienie.

Odpowiedź Zamawiającego:

Zamawiający zmienia treść SIWZ i w Załącznika nr 7 do SIWZ (SOPZ) (Tabela 11 pozycja 5) oraz w Załączniku nr 1A do SIWZ (Tabela 11 pozycja 5) zmienia dotychczasową treść zdania pierwszego, poprzez dopisanie na końcu słów: do obsługi dysków HDD".

Pytanie nr 6:

Dotyczy 8.8. Pamięć obiektowa – pkt 12. Wymagane jest wyposażenie pamięci obiektowej w interfejsy NFS oraz CIFS. Czy Zamawiający dopuści rozwiązanie pozbawione tego typu interfejsów? Wiodące rozwiązania pamięci obiektowej wyposażone są wyłącznie w interfejs S3 (lub inny dedykowany do obsługi obiektów jak WebDAV, REST itp.). Pragniemy zwrócić uwagę Zamawiającego na fakt, iż wykorzystanie macierzy poza jej podstawowym przeznaczeniem (macierz obiektowa) np. do udostępniania danych po NFS oraz CIFS mija się z podstawowym przeznaczeniem macierzy i może powodować niepożądaną degradację jej podstawowych funkcji (obsługa danych obiektowych).

Odpowiedź Zamawiającego:

Zamawiający dopuści rozwiązanie wyposażone wyłącznie w interfejs S3 (lub inny dedykowany do obsługi obiektów jak np. WebDAV, REST). Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 12 pozycja 12) oraz Załącznika nr 1 A do SIWZ (Tabela 12 pozycja 12). Dotychczasowa treść zdania pierwszego otrzymuje brzmienie: „Rozwiązanie musi być wyposażone w możliwość komunikacji i integracji z innymi systemami za pomocą protokołu S3, dodatkowo rozwiązanie może posiadać protokoły plikowe (NFS, CIFS)."

Pytanie nr 7:

Dotyczy 8.9.2. Oprogramowanie do wirtualizacji. Zamawiający specyfikuje wymagania na oprogramowanie do wirtualizacji pomijając zupełnie wymagania na konsolę do zarządzania. Czy Zamawiający dopuści taką wersję konsoli, która obsłuży tylko oprogramowanie dostarczone w ramach niniejszego postępowania?

Odpowiedź Zamawiającego:

Zamawiający wymagania min. odnośnie konsoli zarządzającej środowiskiem wirtualizacyjnym opisał w punkcie 23. Konsola nie może być zamknięta na obsługę jedynie oprogramowania dostarczonego w ramach niniejszego postępowania.

Pytanie nr 8:

Dotyczy 8.10. Zasilacze UPS. Zamawiający w wymaganiach na zasilacze UPS dwukrotnie przywołuje „dostarczane szafy rack" nie specyfikując wymagań ani ilości szaf rack. Prosimy o wyjaśnienia.

Odpowiedź Zamawiającego:

Zamawiający nie wymaga w ramach postepowania dostarczenia szafy rack. Jednocześnie Zamawiający zmienia zapisy w Załączniku nr 7 do SIWZ (Tabela 16 pozycja 2 c) oraz w Załączniku nr 1 A do SIWZ (Tabela 16 pozycja 2 c). Pozycja 2 litera c) otrzymuje brzmienie: „UPS musi zostać połączony w sposób zapewniający zasilanie awaryjne co najmniej na jednej linii zasilania dochodzącej do posiadanej przez Zamawiającego szafy rack".

Pytanie nr 9:

Dotyczy 8.9.3.5. Oprogramowanie do automatyzacji. Czy Zamawiający dopuści potwierdzenie spełnienia wymagań w zakresie sprzętu poprzez deklarację Wykonawcy (platforma automatyzacji nie ma listy wspieranego sprzętu a jedynie oprogramowania systemowego na którym działa)? Alternatywnie, czy Zamawiający uzna wymaganie za spełnione jeżeli wskazana zostanie lista wsparcia dostarczonego sprzętu dla oprogramowania Vmware, na którym uruchomione będzie środowisko automatyzacji?

Odpowiedź Zamawiającego:

Zamawiający uzna za spełnienie wymagań dla listy oprogramowania systemowego na którym działa.

Pytanie nr 10:

Dotyczy 8.8. Pamięć masowa – obiektowa – pkt 2. Systemy pamięci obiektowej charakteryzują się zabezpieczeniem na poziomie danych (obiektów), to znaczy umożliwiają przechowywanie obiektu w kilku niezależnych kopiach, gdzie każda kopia składowana jest na fizycznie niezależnym od pozostałych węźle. W sytuacji gdy obiekt przechowywany jest w trzech kopiach nawet w przypadku awarii dwóch fizycznych węzłów (urządzeń) utrzymywany jest dostęp do danych. Zabezpieczenie polegające na odporności na awarię dwóch dysków nie umożliwia takiej funkcjonalności. Czy Zamawiający dopuści rozwiązanie gwarantujące odporność systemu na awarię dwóch węzłów/urządzeń logicznych zamiast odporności na awarię dwóch dysków?

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy w punkcie 2, informując jednocześnie, że wymaga, aby każdy obiekt zapisywany był w minimum trzech kopiach lub może być zapisany w sposób zapewniający odporność na awarię dwóch dowolnych dysków jednocześnie.

Pytanie nr 11:

Dotyczy 8.8. Pamięć masowa – obiektowa – pkt 4 Czy Zamawiający wymaga dostarczenia dodatkowych dwóch wkładek SFP+ ponad wkładki dostarczane w ramach urządzenia?

Odpowiedź Zamawiającego:

Zamawiający nie wymaga dostarczenia dodatkowych wkładek, tylko minimum dwóch wkładek z urządzeniem na potrzeby dołączenia do infrastruktury.

Pytanie nr 12:

Dotyczy 8.8. Pamięć masowa – obiektowa – pkt 22. Zamawiający wymaga aby wsparcie techniczne świadczył producent oraz polski dystrybutor lub partner serwisowy. Wsparcie techniczne (udostępnianie poprawek, nowych wersji oprogramowania, przewodników konfiguracyjnych etc.) jest w przypadku każdego producenta zapewniane przez tego właśnie producenta (specjalne portale producenta) a nie przez dystrybutora czy też partnera serwisowego. Wymaganie zdaniem Wykonawcy jest nadmiarowe i służyć może jedynie ograniczeniu możliwych do zaoferowania Zamawiającemu rozwiązań. Czy Zamawiający dopuści zaoferowanie rozwiązania wraz z odpowiednią (zawierająco wszystkie wymagane w

pkt. 8.8. ppkt 22 usługi) świadczone zgodnie z przyjętą na rynku IT praktyką przez producenta oferowanego rozwiązania oraz na warunkach opisanych w załączniku nr 8 do SIWZ (Istotne postanowienia umowy)? Pragniemy dodatkowo zwrócić Zamawiającemu uwagę na niezgodność cytowanych powyżej zapisów z np. postanowieniami załącznika nr 8 do SIWZ (istotne postanowienia umowy) gdzie Zamawiający w par. 10 ust. 6 pkt 1 d i e odwołuje się bezpośrednio do stron producenta.

Odpowiedź Zamawiającego:

Zamawiający wykreśla możliwość wsparcia świadczonego przez polskigo dystrbutora.
Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 12 pozycja 22) oraz Załącznika nr 1 A do SIWZ (Tabela 12 pozycja 22). Pozycja 22 otrzymuje brzmienie: „Wraz z urządzeniem wymagane jest zapewnienie opieki technicznej ważnej przez okres 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta lub Certyfikowanego Partnera Serwisowego Producenta, wsparcie w trybie Next Business Day, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
W przypadku awarii dyski pozostają u Zamawiającego."

Pytanie nr 13:

Dotyczy 8.11 System backupu. - Zamawiający specyfikując wymagania na system backupu specyfikuje wymagania na wszystkie komponenty poza platformą serwerową. Czy Zamawiający udostępni platformę serwerową pod system backup?

Odpowiedź Zamawiającego:

Zamawiający udostępni platformę, w ramach której zostanie zainstalowane oprogramowanie systemu backupu. Wykonawca musi dostarczyć wszystkie niezbędne licencje do instalacji całości systemu backupu wraz z licencją systemu operacyjnego oraz 3 letnim wsparciem technicznym świadczonym przez Producenta lub Certyfikowanego Partnera Serwisowego Producenta.

Pytanie nr 14:

Dotyczy 8.1 Przełączniki rdzeniowe – pkt 22. Zamawiający wymaga urządzenia które musi obsługiwać routing między sieciami VLAN – routing statyczny oraz protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP. W rozwiązaniach różnych producentów

wymieniony protokoły wymagają dodatkowej licencji. Czy zamawiający zaakceptuje rozwiązanie w ramach którego uruchomienia protokołów IS-IS oraz BGP wymaga dostarczenia dodatkowej licencji nie będącej przedmiotem postępowania? Pozwoli to optymalizację kosztów całego rozwiązania oraz możliwość w przyszłość wykorzystania protokołów IS-IS i BGP (poprzez zastosowanie odpowiednich licencji) przy rozbudowach.

Odpowiedź Zamawiającego:

Zamawiający w ramach postępowania zaakceptuje przedstawione wyżej wymienione rozwiązanie i nie wymaga dostarczenia dodatkowych licencji dot. protokołów IS-IS oraz BGP.

Pytanie nr 15:

Dotyczy 8.2 Przełącznik 48 portowy – pkt 5. Zamawiający wymaga możliwość rozbudowy o co najmniej 2 porty o prędkości co najmniej 10Gb/s. Czy Zamawiający uzna warunek za spełniony jeśli w zaoferowany przełącznik będzie posiadał już wbudowany dwa porty uplink o prędkości co najmniej 10Gb/s ponad wskazane w pkt 2 i pkt. 4.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy SOPZ. Przełącznik ma mieć możliwość w przyszłości rozbudowy o dwa porty 10Gb/s lub 40Gb/s.

Pytanie nr 16:

Dotyczy 8.3 Przełącznik 48 portowy (DataCenter) – pkt 22. Zabawiający wymaga urządzenia które musi obsługiwać routing między sieciami VLAN – routing statyczny oraz protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP. W rozwiązaniach różnych producentów wymieniony protokoły wymagają dodatkowej licencji. Czy zamawiający zaakceptuje rozwiązanie w ramach którego uruchomienia protokołów IS-IS oraz BGP wymaga dostarczenia dodatkowej licencji nie będącej przedmiotem postępowania? Pozwoli to optymalizację kosztów całego rozwiązania oraz możliwość w przyszłość wykorzystania protokołów IS-IS i BGP (poprzez zastosowanie odpowiednich licencji) przy rozbudowach.

Odpowiedź Zamawiającego:

Zamawiający w ramach postępowania zaakceptuje przedstawione wyżej wymienione rozwiązanie i nie wymaga dostarczenia dodatkowych licencji dot. protokołów IS-IS oraz BGP.

Pytanie nr 17:

Dotyczy 8.4.4 Punkt dostępowy wraz z oprogramowaniem- pkt 26. Zamawiający wymaga punkt dostępowy posiadający 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.9 dBi dla pasma 5 GHz. Czy Zamawiający dopuści punkty dostępowe posiadające 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.8 dBi dla pasma 5 GHz. Zmiana taka może istotnie obniżyć koszty dostarczonych punktów dostępowych.

Odpowiedź Zamawiającego:

Zamawiający dopuszcza punkty dostępowe posiadające 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.8 dBi dla pasma 5 GHz. Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 8 pozycja 26) oraz Załącznika nr 1 A do SIWZ (Tabela 8 pozycja 26). Pozycja 26 otrzymuje brzmienie: „Punkt dostępowy musi posiadać 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.9 dBi dla pasma 5 GHz lub punkt dostępowy posiadający 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.8 dBi dla pasma 5 GHz".

Pytanie nr 18:

Dotyczy 8.5 Zapora sieciowa NGFW – pkt 47. Zamawiający wskazał różne typy plików mających spełniać wymaganie. Z uwagi że pliki JPG nie są plikami „aktywnymi" (ideą systemów sand-box jest badanie aktywnych plików). Prosimy o usunięcie typu plików JPG z wymagania.

Odpowiedź Zamawiającego:

Zamawiający wykreśla w tabeli nr 9 Minimalne wymagania dla zapory sieciowej NGFW w wierszu 47 słowo „jpg". Zamawiający zmienia treść Załączniku nr 7 do SIWZ (SOPZ) (Tabela 9 pozycja 47) oraz Załącznika nr 1 A do SIWZ (Tabela 9 pozycja 47). Pozycja 47 otrzymuje

brzmienie: „System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus, czyli nie mniej niż 3 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."

Pytanie nr 19:

Wykonawca zwraca się z zapytaniem o możliwość usunięcia oświadczenia zawartego w §2 ust. 1 pkt 3 o treści: „dostarczone i wdrożone przez niego rozwiązania nie będą posiadać żadnych ukrytych/nieudokumentowanych mechanizmów, mogących mieć wpływ na bezpieczeństwo i ponosi w tym zakresie pełną odpowiedzialność" – z uwagi na fakt iż Wykonawca dołoży najwyższych starań aby wdrożyć takie rozwiązanie, jednak osiągnięcie sytuacji pełnego braku wpływu może w jednostkowych przypadkach być nie zawsze możliwe. Wszystko to jednak bez istotnego wpływu na funkcjonowanie systemu."

Odpowiedź Zamawiającego:

Zamawiający zmienia treść §2 ust. 1 pkt 3 załacznika nr 8 do SIWZ i otrzymuje on brzmienie: „dostarczone i wdrożone przez niego rozwiązania nie będą posiadać żadnych ukrytych / nieudokumentowanych mechanizmów znanych Wykonawcy, mogących mieć wpływ na bezpieczeństwo.".

Pytanie nr 20:

Wykonawca zwraca się z zapytaniem o możliwość uzupełnienia zapisu § 2 ust. 2 pkt 2 Umowy o końcową klauzulę w myśl której „zmiana wskazanych poprzednio dokumentów nie może podnosić kosztów wykonania umowy przez Wykonawcę", w celu zabezpieczenia ekwiwalentności świadczeń obu stron.

Odpowiedź Zamawiającego:

Zamawiający zmienia treść § 2 ust. 2 pkt 2 załacznika nr 8 do SIWZ, poprzez dodanie na końcu słów: „przy czym zmiana ww. wskazanych dokumentów nie będzie powodowała dodatkowych kosztów wykonania umowy po stronie Wykonawcy,".

Pytanie nr 21:

Wykonawca zwraca się z zapytaniem o możliwość wydłużenia terminu wskazanego w §3 ust. 8 umowy do .... Dni roboczych, z uwagi na to iż przewidziany pierwotnie termin 3 dni roboczych jest zbyt krótki z uwagi na skalę obowiązków operacyjnych Wykonawcy.

Odpowiedź Zamawiającego:

Zamawiający zmienia termin wskazany w §3 ust. 8 załacznika nr 8 do SIWZ na 5 dni roboczych.

Pytanie nr 22:

Wykonawca zwraca się z zapytaniem o możliwość skrócenia okresu rękojmi na przedmiot umowy, wynikającej z §10 - do okresu 3 lat, z uwagi na to iż cykl życia technicznego danego produktu oraz jego wsparcia może nie być odpowiednio długi dla racjonalnego kosztowo spełnienia ww. zapisu umowy.

Odpowiedź Zamawiającego:

Zamawiający w §10 ust. 1 pkt. 2 zmienia okres rękojmi za wady na Przedmiot Umowy na okres równy 3 lat.

Pytanie nr 23:

Wykonawca zwraca się z zapytaniem o jaką dokumentacje chodzi w zapisie §11 ust.2 pkt 1 Umowy – czy jest to dokumentacja powykonawcza?"

Odpowiedź Zamawiającego:

Zamawiający poprzez „Dokumentację" wskazaną w § 11 ust.2 pkt 1 załacznika nr 8 do SIWZ rozumie dokumentację każdorazowo wytworzoną przez Wykonawcę na potrzeby realizacji przedmiotowej Umowy.

Pytanie nr 24:

Wykonawca zwraca się z zapytaniem o możliwość zmiany zapisu § 12 ust 1 pkt. 2 Umowy poprzez jego uzupełnienie o zapis wskazujący minimalną oraz maksymalną długość terminu dodatkowego, wyznaczonego przez Zamawiającego dla naprawienia zaniedbania – po upływie którego Zamawiający może odstąpić od umowy. Umowa nie określa tego terminu a okoliczności minimalne winny być wskazane.

Odpowiedź Zamawiającego:

Zamawiający zmienia treść §12 ust. 1 pkt. 2 poprzez określenie terminu na 14 dni kalendarzowych.

Pytanie nr 25:

Wykonawca zwraca się z zapytaniem o możliwość dokonania zmiany zapisów §13 ust. 1 pkt. 2 umowy poprzez wprowadzenie stawki procentowej ustalania wysokości kar umownych w odniesieniu do wartości wynagrodzenia umownego w wysokości 0,2% za każdy dzień zwłoki w miejsce kary określonej kwotowo, oraz zmiany zapisów §13 ust.1 pkt. 3 do 8- w wysokości 0,1% wartości wynagrodzenia za każdy dzień zwłoki, w miejsce określonych w tych zapisach stawek kwotowych. Takie ustalenie wysokości kar umownych jest bardziej przejrzyste i obiektywnie umożliwiające porównanie zapisów umowy do typowego poziomu kar umownych określanych w umowach zawieranych w celu realizacji zamówień publicznych.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje dotychczasowe zapisy załącznika nr 8 do SIWZ.

Pytanie nr 26:

Wykonawca zwraca się z zapytaniem o możliwość wydłużenia przewidzianego w § 13 ust. 7 zaledwie 2 dniowego terminu na zgłoszenie powiadomienia o zaistnieniu siły wyższej. Proponowany w umowie 2 dniowy termin jest zbyt krótki dla zapewnienia realnej możliwości skorzystania przez Wykonawcę z instytucji siły wyższej. Wykonawca proponuje wydłużenie tego terminu do 5 dni roboczych, który jest bardziej adekwatny do ogólnych możliwości utrzymywania kontaktu przez strony w okresie występowania siły wyższej.

Odpowiedź Zamawiającego:

Zamawiający zmienia treść §13 ust. 7 Załącznika nr 8 do SIWZ i zmienia termin powiadamiania o zainstnieniu siły wyższej na 5 dni roboczych.

Pytanie nr 27:

Wykonawca zwraca się z zapytaniem o możliwość usunięcia par. 14 ust 3 pkt 3 oraz ust. 7 jako bardzo niekorzystnych dla Wykonawcy, przerzucających na Wykonawcę ryzyko zmian organizacyjnych przeprowadzanych przez Zamawiającego we własnej strukturze. Wykonawca nie ma na nie jakiegokolwiek wpływu i nie powinien ponosić negatywnych konsekwencji z tym związanych.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy załącznika nr 8 do SIWZ z uwagi na fakt, iż zgodnie z §14 ust. 15 ww. załącznika „wszelkie zmiany w umowie wymagają formy pisemnej w postaci anekesu pod rygorem nieważności".

Pytanie nr 28:

Wykonawca zwraca się z zapytaniem o możliwość skrócenia okresu zachowania poufności określonego w par. 16 ust. 7 – jako 10 lat od daty wygaśnięcia umowy, co jest rozwiązaniem stanowczo za długim, do standardowego zapisu przewidującego 5 letni okres liczony od daty wygaśnięcia umowy.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje dotychczasowe zapisy załacznika nr 8 do SIWZ.

Pytanie nr 29:

Wykonawca zwraca się z zapytaniem o możliwość zmiany zapisu par. 17 ust. 2 i 3 poprzez uzupełnienie ww. przepisów tak aby przewidywały obowiązek zwrotu kwot zabezpieczenia pieniężnego wraz z oprocentowaniem wynikającym z lokat bankowych.

Odpowiedź Zamawiającego:

Obowiązek zwrotu zabezpieczenia należytego wykonania umowy realizowany będzie przez Zamawiającego zgodnie z treścią art. 148 ust. 5 ustawy Pzp.

Pytanie nr 30:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 11, Zamawiający wymaga: "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." Podane zapisy szczegółowo wskazują wyłącznie na producenta Palo Alto Networks. Prosimy o dopuszczenie rozwiązania, w którym Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje dotychczasowe zapisy Załącznika nr 8 do SIWZ.

Pytanie nr 31:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 19, Zamawiający wymaga: "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, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif lub blokowane plików w wiadomościach email: 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.. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia". Prosimy o potwierdzanie, iż typ pliku „ignored" jest błędem pisarskim i można go pominąć.

Odpowiedź Zamawiającego:

Zamawiający potwierdza wystąpienie oczywistej omyłki pisarskiej i usuwa z zapisów pozycji 19 w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW słowo „ignored".

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 9 pozycja 19) oraz Załącznika nr 1 A do SIWZ (Tabela 9 pozycja 19). Pozycja 19 otrzymuje brzmienie: „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, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif lub blokowane plików w wiadomościach email: 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, unknown, mpeg, mov, mp3, wma, wav, pdf, avi, rm, torrent oraz dodatkowo umożliwia wykorzystanie tworzenia sygnatur IPS do plików nie będących na wymaganej liście. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia."

Pytanie nr 32:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 34, Zamawiający wymaga: "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." Podane zapisy szczegółowo wskazują wyłącznie na producenta Palo Alto Networks. Prosimy o dopuszczenie rozwiązania o następującej treści: "System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp 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."

Odpowiedź Zamawiającego:

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 9 pozycja 34) oraz Załącznika nr 1 A do SIWZ (Tabela 9 pozycja 34). Pozycja 34 otrzymuje brzmienie: „System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp 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".

Pytanie nr 33:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 39, Zamawiający wymaga: "System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń". Podane zapisy szczegółowo wskazują wyłącznie na producenta Palo Alto Networks. Czy Zamawiający uzna poniższe wymaganie za alternatywne gdzie: ochrona anty-spyware odbywa się w module antywirus bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur antywirus zawierająca również sygnatury anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń?

Odpowiedź Zamawiającego:

Zamawiający uzna poniższe wymaganie za alternatywne gdzie: ochrona anty-spyware odbywa się w module antywirus bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur antywirus zawierająca również sygnatury anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 9 pozycja 39) oraz Załącznika nr 1 A do SIWZ (Tabela 9 pozycja 39). Pozycja 39 otrzymuje brzmienie: „System zabezpieczeń firewall musi posiadać moduł anty-spyware lub może zawierać się w module antywirus bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu jako niezależna baza lub może

zawierać się w module antywirus, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń".

Pytanie nr 34:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 49, Zamawiający wymaga: "49 Administrator musi mieć możliwość konfiguracji rodzaju pliku poddanego analizie typu „Sand-Box"." Podane zapisy szczegółowo wskazują wyłącznie na producenta Palo Alto Networks. Prosimy o dopuszczenie rozwiązania, które pozwala na skonfigurowanie wysyłania do skanowania prze Sand-Box wszystkich wspieranych plikow i e.w. dodanie wyjątków, które pliki mają być wyłączone ze skanowana przez Sand-box (np. exe, msoffice, java, jpeg, zip, rar, tar, bat, pdf, inne).

Odpowiedź Zamawiającego:

Zamawiający uzna za wymaganie alternatywne wysyłanie do skanowania przez Sand-Box wszystkich wspieranych plików i e.w. dodanie wyjątków, które pliki mają być wyłączone ze skanowana przez Sand-box (np. exe, msoffice, java, jpeg, zip, rar, tar, bat, pdf, inne)

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 9 pozycja 49) oraz Załącznika nr 1 A do SIWZ (Tabela 9 pozycja 49). Pozycja 49 otrzymuje brzmienie: „Administrator musi mieć możliwość konfiguracji rodzaju pliku poddanego analizie typu „Sand-Box" lub mieć możliwość wysyłania do skanowania przez „Sand-Box" wszystkich wspieranych plików i e.w. dodanie wyjątków, które pliki mają być wyłączone ze skanowana przez Sand-box (np. exe, msoffice, java, jpeg, zip, rar, tar, bat, pdf, inne)".

Pytanie nr 35:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 56, Zamawiający wymaga: "System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci" Prosimy o potwierdzenie że możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci należy rozumieć jako weryfikacje przed przyznaniem dostępu przy połączeniu zdalnym SSVPN.

Odpowiedź Zamawiającego:

Zamawiający wymaga funkcjonalności opisanej w punkcie 56 dla IPSec oraz SSLVPN dla min. 500 użytkowników.

Pytanie nr 36:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 57, Zamawiający wymaga: "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" Prosimy o usunięcie wymagania gdyż wymaganie w takiej postaci może być spełnione wyłącznie przez rozwiązania producenta Palo Alto Networks lub prosimy o dopuszczenie rozwiązania, które na etapie dostarczenia nie obsługuje mechanizmu uwierzytelnienia SAML 2.0 lecz posiada możliwość rozbudowy w razie potrzeby w przyszłości.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy SOPZ.

Pytanie nr 37:

W punkcie 70 Zamawiający dopuszcza rozwiązanie, w którym logi przechowywane w są centralnym systemie przechowywana logów. Prosimy o dopuszczenie rozwiązania, gdzie funkcjonalność opisana w pkt. 76 będzie realizowana w centralnym systemie przechowywana logów.

Odpowiedź Zamawiającego:

Zamawiający zaakceptuje funkcjonalności opisane w punkcie 76 przechowywane bezpośrednio na urządzeniu lub w centralnym systemie logowania producenta urządzenia w postaci dedykowanej VM.

Pytanie nr 38:

W punkcie 70 Zamawiający dopuszcza rozwiązanie, w którym logi przechowywane w są centralnym systemie przechowywana logów. Prosimy o dopuszczenie rozwiązania, gdzie funkcjonalność opisana w pkt. 71 będzie realizowana w centralnym systemie przechowywana logów.

Odpowiedź Zamawiającego:

Zamawiający zaakceptuje funkcjonalności opisane w punkcie 71 przechowywane bezpośrednio na urządzeniu lub w centralnym systemie logowania producenta urządzenia w postaci dedykowanej VM.

Pytanie nr 39:

W punkcie 70 Zamawiający dopuszcza rozwiązanie, w którym logi przechowywane w są centralnym systemie przechowywana logów. Prosimy o dopuszczenie rozwiązania, gdzie funkcjonalność opisana w pkt. 77 będzie realizowana w centralnym systemie przechowywana logów.

Odpowiedź Zamawiającego:

Zamawiający zaakceptuje funkcjonalności opisane w punkcie 77 przechowywane bezpośrednio na urządzeniu lub w centralnym systemie logowania producenta urządzenia w postaci dedykowanej VM.

Pytanie nr 40:

W rozdziale „8.5 Zapora sieciowa NGFW" OPZ w tabeli 9 „Minimalne wymagania dla zapory sieciowej NGFW w punkcie 29, Zamawiający wymaga: "System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku, gdy analizowany ruch przechodzi

wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. " Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Prosimy o uproszczenie zapisu, gdzie wystarczającym będzie rozpoznawanie adresów z nagłówków XFF, a uwierzytelniania użytkownika dopuszczalne będzie per sesja.

Odpowiedź Zamawiającego:

Zamawiający akceptuje uproszczenie zapisu wyspecyfikowanej funkcjonalności gdzie realizowane będzie rozpoznawanie adresów z nagłówków XFF, a uwierzytelniania użytkownika realizowane będzie per sesja.

Pytanie nr 41:

W rozdziale „8.6 Zapora sieciowa – oddziałowa" OPZ w tabeli 10 „Minimalne wymagania dla zapory sieciowej oddziałowej" w punkcie 1, Zamawiający wymaga: "Urządzenie musi być wyposażone w co najmniej 2 GB pamięci RAM, pamięć Flash 4 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym." Prosimy o dopuszczenie rozwiązania posiadającego 1,82 GB RAM oraz 3,66 GB flash.

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje dotychczasowe zapisy Załącznika nr 8 do SIWZ.

Pytanie nr 42:

W rozdziale „8.6 Zapora sieciowa – oddziałowa" OPZ w tabeli 10 „Minimalne wymagania dla zapory sieciowej oddziałowej" w punkcie 11, Zamawiający wymaga: "Urządzenie musi obsługiwać co najmniej 1000 sieci VLAN z tagowaniem 802.1Q." Prosimy o dopuszczenie rozwiązania obsługującego 256 sieci VLAN z tagowaniem 802.1Q.

Odpowiedź Zamawiającego:

Zamawiający dopuszcza rozwiązanie obsługujące 256 sieci VLAN z tagowaniem 802.1Q.

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 10 pozycja 11) oraz Załącznika nr 1 A do SIWZ (Tabela 10 pozycja 11). Pozycja 11 otrzymuje brzmienie: „Urządzenie musi obsługiwać co najmniej 256 sieci VLAN z tagowaniem 802.1Q."

Pytanie nr 43:

Dotyczy Zapora sieciowa NGFW

Czy Zamawiający przewiduje, że zamawiana para urządzeń NGFW będzie pracowała w klastrze?

Odpowiedź Zamawiającego:

Zamawiający wymaga, aby dwa dostarczone urządzenia działały w klastrze.

Pytanie nr 44:

Dotyczy Zapora sieciowa NGFW

Czy Zamawiający dopuszcza instalowanie systemu zarządzania, logowania i raportowania w postaci maszyny wirtualnej na swojej infrastrukturze?

Odpowiedź Zamawiającego:

Zamawiający zgadza się na dostarczenie przez Wykonawcę systemu zarządzania, logowania i raportowania w postaci maszyny wirtualnej producenta zapory sieciowej NGFW uruchomionej w infrastrukturze Zamawiającego. Dostarczone licencję na system zarządzania, logowania i raportowania powinny zapewniać Zamawiającemu korzystanie z nich przynajniej przez okres gwarancji zaproponowanego urządzenia fizycznego.

Pytanie nr 45:

Dotyczy Zapora sieciowa NGFW

Zamawiający w pkt. 13 wymaga „Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole, gdzie definiowane są aplikacje i oddzielne pole, gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile". Czy Zamawiający usunie zapis "nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile" i dopuści możliwość zastosowania rozwiązania, gdzie alternatywnie stosuje się zaawansowany profil aplikacyjny z granularną kontrolą parametrów?

Odpowiedź Zamawiającego:

Zamawiający wyraża zgodę.

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 9 pozycja 13) oraz Załącznika nr 1 A do SIWZ (Tabela 9 pozycja 13). Pozycja 13 otrzymuje brzmienie: „Zezwolenie

dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole, gdzie definiowane są aplikacje i oddzielne pole, gdzie definiowane są protokoły sieciowe). Zamawiający dopuszcza możliwość zastosowania rozwiązania, gdzie alternatywnie stosuje się zaawansowany profil aplikacyjny z granularną kontrolą parametrów".

Pytanie nr 46:

Dotyczy Zapora sieciowa NGFW

Zamawiający w pkt. 18 wymaga „System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja lub jako parametr polityki dla których dowiązuje się profile ochronne AV, DNS, IPS." Czy zaakceptowane będzie rozwiązanie, gdzie możliwe do zastosowania profile ochronne to AV, IPS, AS, filtr URL, filtr rodzajów plików, filtr DNS oraz profil aplikacyjny z funkcją granularnej kontroli parametrów?

Odpowiedź Zamawiającego:

Zamawiający akceptuje takie rozwiązanie.

Pytanie nr 47:

Dotyczy Zapora sieciowa NGFW

Zamawiający w pkt. 48 wymaga „Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, pomiędzy publicznym i prywatnym systemem typu "Sand-Box". Czy Zamawiający dopuści wybór per urządzenie czy ma korzystać z publicznego czy lokalnego sandboxa?

Odpowiedź Zamawiającego:

Zamawiający dopuści rozwiązanie, w którym administrator będzie mógł podjąć dezycję per urządzenie i będzie miał możliwość korzystania z publicznego lub lokalnego sandboxa.

Pytanie nr 48:

Dotyczy Zapora sieciowa – oddziałowa

Zamawiający w pkt. 5 wymaga „Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 256 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 100 Mb/s IMIX." Czy Zamawiający dopuści rozwiązanie wspierające 200 tuneli Gateway-to-Gateway i 250 tuneli Client-to-Gateway, gdzie wydajność szyfrowania wynosi ponad 4 Gbps?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza takie rozwiązanie.

Pytanie nr 49:

Dotyczy Punkt dostępowy wraz z oprogramowaniem

Czy Zamawiający dopuści punkty dostępowe o uzysku na poziomie 3.3dBi dla pasma 2.4GHz oraz 5.8dBi dla pasma 5GHz?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza punkty dostępowe posiadające 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.8 dBi dla pasma 5 GHz. Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 8 pozycja 26) oraz Załącznika nr 1 A do SIWZ (Tabela 8 pozycja 26). Pozycja 26 otrzymuje brzmienie: „Punkt dostępowy musi posiadać 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.9 dBi dla pasma 5 GHz lub punkt dostępowy posiadający 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 3,3 dBi dla pasma 2,4 Ghz oraz 5.8 dBi dla pasma 5 GHz"

Pytanie nr 50:

Dotyczy Serwery wraz z oprogramowaniem

Czy Zamawiający umieszczając w punkcie 5 „Pamięć operacyjna" zapis „Łączna ilość zainstalowanej pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 7.5 TB" ma na myśli pamięć jaka jest możliwa do zainstalowania w oferowanym serwerze, ale nie jest to pamięć jaka ma być zainstalowana i dostarczona w ramach postępowania?

Jeżeli tak, to czy Zamawiający dopuści serwer z możliwością instalacji pamięci persistent memory oraz pamięci RDIMM lub LRDIMM o łącznej pojemności do 7.5 TB?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza serwer z możliwością instalacji pamięci persistent memory oraz pamięci RDIMM lub LRDIMM o łącznej pojemności do 7.5 TB.

Pytanie nr 51:

Dotyczy Serwery wraz z oprogramowaniem

Czy Zamawiający dopuści serwer bez możliwości przewidywania awarii dla regulatorów napięcia?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza tego typu rozwiązanie.

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 13 pozycja 19) oraz Załącznika nr 1 A do SIWZ (Tabela 13 pozycja 19). Pozycja 19 otrzymuje brzmienie: „Możliwość przewidywania awarii dla procesorów, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.

Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera."

Pytanie nr 52:

Dotyczy Serwery wraz z oprogramowaniem

Czy Zamawiający dopuści serwer wyposażony w kartę sieciową z dodatkowymi dwoma portami 10Gb SFP+ wymaganą w punkcie 11 interfejsy sieciowe bez wsparcia dla DCB oraz bez możliwości realizacji bezpośredniego dostępu do pamięci iWARP?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza tego typu rozwiązanie.

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 13 pozycja 11) oraz Załącznika nr 1 A do SIWZ (Tabela 13 pozycja 11). Pozycja 11 otrzymuje brzmienie: „Zintegrowane na płycie głównej 2 porty 10Gb SFP+ wyposażone we wkładki typu SR lub kable

DAC. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w punkcie Dodatkowe sloty I/O .

Wymagana funkcjonalność wbudowanych portów:

NIC teaming, możliwość realizacji bezpośredniego dostępu do pamięci iWARP, SR-IOV, offload sumy kontrolnej stosu TCP/IP, obsługa ramek Jumbo do 9.5Kb lub podział portu 10Gb na 4 porty wirtualne, obsługa VXLAN/NVGRE, wsparcie dla VMware NetQue / VMQ oraz Microsoft VMQ & Dynamic VMQ, obsługa ramek Jumbo do 9200b, wymagana funkcjonalność RDMA, wymagana możliwość aktywowania pełnego sprzętowego wsparcia dla FCoE / iSCSI

Dodatkowe dwa porty SFP+ wyposażone we wkładki typu SR lub kable DAC zainstalowane na karcie rozszerzeń.

Wymagana funkcjonalność tych portów: wymagana funkcjonalność podziału portu 10Gb na 4 porty wirtualne, obsługa VXLAN/NVGRE, wsparcie dla VMware NetQue / VMQ oraz Microsoft VMQ & Dynamic VMQ, obsługa ramek Jumbo do 9200b, wymagana funkcjonalność RDMA, wymagana możliwość aktywowania pełnego sprzętowego wsparcia dla FCoE / iSCSI lub NIC teaming, SR-IOV, offload sumy kontrolnej stosu TCP/IP, obsługa ramek Jumbo do 9.5Kb

Wraz z urządzeniem Wykonawca dostarczy minimum 4 wkładki SFP+ (10 Gb multimode) lub kable AOC (min. 2m) lub kable DAC (min. 2m) jeżeli dostarczone urządzenia pochodzą od tego samego producenta co zaproponowane przełączniki typy Data Center.

Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej."

Pytanie nr 53:

Dotyczy Przełączniki rdzeniowe, Przełącznik 48 portowy – dostępowy, Przełącznik 48 portowy (DataCenter)

Czy wkładki dostarczone wraz z przełącznikami mają być oryginalne i pochodzić od producenta dostarczanych przełączników?

Odpowiedź Zamawiającego:

Zamawiający wymaga, aby wszystkie wkładki były oryginalne i znajdowały się na liście kompatybilności producenta urządzenia. Jednoczśenie Zamawiający informuje, że takie wymaganie zawarł załaczniku nr 7 do SIWZ w rozdziale 8 Dostawa infrastruktury i programowania, pkt 7 dla wszystkich urządzeń.

Pytanie nr 54:

Dotyczy Kontrolery WiFi, System zarządzania

Czy Zamawiający wymaga, aby kontrolery WiFi z punktu 8.4.1 i system zarządzania z punktu 8.4.2 były objęte gwarancją analogiczną jak Arbiter dla kontrolerów z punktu 8.4.3. to jest: „Minimum 3-letnia gwarancja producenta obejmująca wszystkie elementy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta"?

Odpowiedź Zamawiającego:

Gwarancją 3-letnią mają być objęte wszystkie elementy rozwiązania dotyczącego systemu WiFi.

Pytanie nr 55:

Dotyczy Serwery wraz z oprogramowaniem

Czy Zamawiający dopuści dodatkowe oprogramowanie zarządzające, które ma możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesłaniem informacji na temat wydarzenia dotyczącego sprzętu lub przesłaniem plików diagnostycznych?

Odpowiedź Zamawiającego:

Zamawiający zaakceptuje funkcjonalność oprogramowania zarządzającego, która ma możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesłaniem informacji na temat wydarzenia dotyczącego sprzętu lub przesłanie plików diagnostycznych. Zamawiający będzie dodatkowo wymagał, aby była możliwość świadomego wyłączenia i włączenia tej funkcjonalności.

Pytanie nr 56:

Dotyczy Serwery wraz z oprogramowaniem

Czy Zamawiający zapisując wymaganie Email Forwarding w opisie na dodatkowe oprogramowanie zarządzające ma na myśli aby dodatkowe oprogramowanie zarządzające pozwalało na wygenerowanie i przesłanie (np. przez zewnętrzny serwer pocztowy) wiadomości email?

Odpowiedź Zamawiającego:

Zamawiający oczekuje od funkcjonalności Email Forwarding wysłania alertu z błędem na adres e-mail, nie wymagana jest funkcjonalność dalszego przysłania wiadomości z wygenerowany alertem, czyli funkcjonalności Forwarding.

Pytanie nr 57:

Zamawiający wymaga kontrolera obsługującego 30 AP z możliwością dalszej rozbudowy do 1000AP. Czy Zamawiający dopuszcza rozbudowę kontrolera poprzez dokładanie kolejnych licencji rozbudowujących maksymalną pojemność kontrolera oraz licencji na liczbę obsługiwanych AP w ramach maksymalnej dostępnej licencyjnie pojemności, czy też maksymalna wymagana pojemność kontrolera ma być dostępna od razu, bez konieczności dokupywania licencji, a rozbudowa ma polegać jedynie na dokładaniu licencji pojemnościowych na liczbę obsługiwanych AP w ramach maksymalnej pojemność kontrolera?

Odpowiedź Zamawiającego:

Zamawiający wymaga aby kontroler wspierał obsługę co najmniej 50 AP (bez konieczności dokładania kolejnych licencji rozszerzających ten zakres i zmian w konfiguracji maszyny wirtualnej) oraz posiadać licencje pozwalające na obsługę co najmniej 30 AP z możliwością dalszej rozbudowy w przyszłości do 1 000 punktów dostępowych poprzez dodanie licencji wirtualnych kontrolerów oraz licencji aktywujących obsługę AP.

Zamawiający zmienia treść Załącznika nr 7 do SIWZ (SOPZ) (Tabela 5 pozycja 2) oraz Załącznika nr 1 A do SIWZ (Tabela 5 pozycja 2). Pozycja 2 otrzymuje brzmienie: „Kontrolery muszą wspierać obsługę co najmniej 50 AP (bez konieczności dokładania kolejnych licencji

rozszerzających ten zakres i zmian w konfiguracji maszyny wirtualnej) oraz posiadać licencje pozwalające na obsługę co najmniej 30 AP z możliwością dalszej rozbudowy w przyszłości do 1 000 punktów dostępowych poprzez dodanie licencji wirtualnych kontrolerów oraz licencji aktywujących obsługę AP."

Zgodnie z treścią art. 38 ust. 4 ustawy Pzp, w związku z ww. zmianami, Zamawiający zmienił treść załacznika nr 1A do SIWZ – Wykaz dostarczanych produktów, załacznika nr 7 do SIWZ – Szczegółowy Opis Przedmiotu Zamówienia i załacznika nr 8 do SIWZ – Istotne postanowienia Umowy oraz zwraca się z prośbą o zapoznanie się z ich treścią.