L. Dz. 119/01/2022 Poznań, 14 stycznia 2022 r.

Do wszystkich Wykonawców

Dotyczy: Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, na podstawie art. 132 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2021 r., poz. 1129). Nr postępowania **PN 22/12/2021 – dostawa NGFW.**

I.

Zamawiający informuje, że w dniu 10.01.2022 r. wpłynął wniosek o wyjaśnienie treści SWZ dotyczącej ww. postępowania o udzielenie zamówienia publicznego, na który Zamawiający zgodnie z art. 135 ust. 2 ustawy Pzp, udziela następujących wyjaśnień:

Pytanie 1.

Zamawiający w odpowiedzi na pytanie 10 z dnia 23/12/2021 określił iż komponent centralny musi umożliwiać automatyczny zapis 20 poprzednich wersji oprogramowania. Bardzo prosimy o informację czy właściwym rozumieniem jest, iż funkcja ta wymagana jest bezpośrednio w urządzeniu firewall będącym w tym przypadku komponentem centralnym, i nie może wymagać wykorzystania systemu zarządzania w celu realizacji tej funkcji (szczególnie ważne jest to w przypadku potencjalnej awarii, o której wspominał Zamawiający w odpowiedzi na pytanie). Jednocześnie prosimy o potwierdzenie, iż Zamawiający oczekuje tutaj funkcji pozwalającej na odtworzenie pełnej konfiguracji urządzenia z każdej dowolnie wybranej wersji zapisanej konfiguracji.

Odpowiedź:

Funkcja automatycznego zapisu minimum 20 poprzednich wersji konfiguracji jest wymagana bezpośrednio w urządzeniu firewall będącym komponentem centralnym i nie może wymagać wykorzystania komponentu zarządczego w celu realizacji tej funkcji.

Zamawiający wymaga funkcjonalności odtworzenia konfiguracji urządzenia z każdej dowolnie wybranej wersji zapisanej konfiguracji.

Tym samym Zamawiający informuje, że w oparciu o art. 137 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2021 r., poz. 1129) zwaną dalej ustawą Pzp , dokonuje zmian treści Specyfikacji Warunków Zamówienia dalej SWZ przed upływem terminu składania ofert.

Dokonane zmiany treści SWZ Zamawiający udostępnia na stronie internetowej prowadzonego postępowania poprzez zamieszczenie ujednoliconej wersji SWZ z zaznaczonymi zmianami w pliku pod nazwą: SWZ_dostawa NGFW_zmiana_SWZ2.pdf

Pytanie 2.

W punkcie 22 Zamawiający określił wymagania dotyczących konfiguracji kandydackiej nie precyzując jednocześnie czy dotyczy to pełnej konfiguracji czy wybranych jej elementów. Bardzo prosimy o informację czy właściwym rozumieniem jest, iż funkcja ta musi obejmować całościową konfigurację

komponentu centralnego i obejmować całościową konfigurację w tym m.in. konfigurację polityk, interfejsów, routingu, dostępu administracyjnego (role/uprawnienia administratorów) oraz inne jej elementy składowe, a także funkcja ta musi umożliwiać weryfikację zmian w konfiguracji i jej sprawdzenie przed zatwierdzeniem jako nowej aktywnej konfiguracji urządzenia.

Odpowiedź:

Zamawiający wymaga, aby przed zatwierdzaniem zmian na urządzeniu była możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej w stosunku do wersji aktywnej. Sposób prezentacji zmian powinien dać administratorowi pełną wiedzę o wprowadzanych zmianach. Ponadto funkcja ta musi umożliwiać sprawdzenie konfiguracji kandydackiej przed jej zatwierdzeniem jako aktywnej konfiguracji urządzenia.

Tym samym Zamawiający informuje, że w oparciu o art. 137 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2021 r., poz. 1129) zwaną dalej ustawą Pzp , dokonuje zmian treści Specyfikacji Warunków Zamówienia dalej SWZ przed upływem terminu składania ofert.

Dokonane zmiany treści SWZ Zamawiający udostępnia na stronie internetowej prowadzonego postępowania poprzez zamieszczenie ujednoliconej wersji SWZ z zaznaczonymi zmianami w pliku pod nazwą: SWZ_dostawa NGFW_zmiana_SWZ2.pdf

Pytanie 3.

W punkcie 4 Zamawiający określił, iż wiążącym dla oceny wydajności urządzeń jest profil ruchu IMIX „Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na poszczególnych systemach zakładają profil całego ruchu typu IMIX (ang. Internet MIX według IETF RFC 6985 „IMIX Genome: Specification of Variable Packet Sizes for Additional Testing”).” Chcielibyśmy zwrócić uwagę, iż parametr ten jest w oderwaniu od parametrów wydajnościowych podawanych dla firewalli następnej generacji, jest on stosowany do testowania urządzeń pracujących w warstwie L3/L4 (routery/przełączniki sieciowe) natomiast urządzenie będące przedmiotem zamówienia jest firewallem działającym w warstwie 7 modelu OSI. Zgodnie bowiem z wskazanym dokumentem RFC możliwe jest określenie, iż ruchem testowym będzie ruch UDP tudzież Echo UDP (port 7), co spowoduje, iż firewalle każdego z liczących się producentów będą mogły uzyskać wymagane przepustowości na platformach znacząco mniejszych niż wymagane – wg nas – w zamyśle przez Zamawiającego. Dlatego też wnosimy o zmianę wymagania w taki sposób, iż wymagana przepustowość będzie musiała zostać uzyskana (a tym samym wymaganie spełnione) dla charakterystyk ruchu podawanych przez producentów w kartach katalogowych a określanych jako „mix ruchu” – w przypadku Fortinet jest to „Enterprise Mix”, dla Checkpoint „Enterprise Testing Conditions”, Palo Alto Networks określa to jako appmix, lub odpowiednik dla producenta oferowanych rozwiązań. Pozwoli to Zamawiającemu na wykluczenie sytuacji w których Wykonawcy będą posługiwali się charakterystykami określanymi jako idealne do przeprowadzenia testów „Ideal Testing Conditions” Proponujemy zmianę zapisu na „Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na poszczególnych systemach zakładają iż będą to parametry określone przez producentów w kartach katalogowych jako Enterprise Mix/Enterprise Testing Conditions/appmix lub odpowiednik właściwy dla producenta oferowanych rozwiązań jako komponentu centralnego, publikowany w oficjalnej karcie katalogowej dla oferowanego urządzenia.

Jednocześnie niedopuszczalne jest przyjmowanie charakterystyk ruchowych określanych jako tzw. „idealne” np. fail-open– bez względu na producenta oferowanych rozwiązań.”

Odpowiedź:

Wszystkie parametry dotyczące wydajności, pod kątem przepustowości (ang. throughput), wymaganej na komponencie centralnym zakładają, iż będą to parametry wskazane przez producentów w kartach katalogowych jako Enterprise Mix/Enterprise Testing Conditions/appmix lub dla równoważnego modelu ruchu. Przy czym przez równoważny model ruchu rozumie się taki ruch:

- dla którego wymagane parametry wydajnościowe są osiągane w ruchu całościowym (up/down) i jednocześnie
- w którym rozkład procentowy ruchu wybranych protokołów wykorzystujących pakiety różnej wielkości, przy pomocy których realizowane są różne aplikacje (np. youtube, facebook, google, gmail, ssh, smtp z załącznikami) jest przedstawiony w tabeli poniżej:

Protokół	**Udział w %**
HTTP	15%
HTTPS	60%
SMTP, IMAP, POP3, FTP, SMB i inne	22%
DNS	3%

Zamawiający dopuszcza odchylenie od przedstawionych wielkości udziałów dla poszczególnych protokołów o 10 punktów procentowych w górę albo w dół.

Tym samym Zamawiający informuje, że w oparciu o art. 137 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2021 r., poz. 1129) zwaną dalej ustawą Pzp , dokonuje zmian treści Specyfikacji Warunków Zamówienia dalej SWZ przed upływem terminu składania ofert.

Dokonane zmiany treści SWZ Zamawiający udostępnia na stronie internetowej prowadzonego postępowania poprzez zamieszczenie ujednoliconej wersji SWZ z zaznaczonymi zmianami w pliku pod nazwą: SWZ_dostawa NGFW_zmiana_SWZ2.pdf

Pytanie 4.

Zamawiający w odpowiedzi na pytanie 1 z dnia 30/12/2021 określił, zaakceptuje rozwiązanie tego samego producenta, na którym logi i konfiguracja będzie przechowywana w systemie Centralnego Zarządzania, z pojemnością dysku 4 TB w RAID 5 . Jednocześnie dla przypadku w którym komponent centralny (Firewall, brama) jest zarządzane w taki sposób, iż jest ono zależne od systemu centralnego zarządzania może zaistnieć sytuacja w której wskutek awarii samego systemu zarządzania (który stanowi pojedynczy punkt awarii) komponent centralny pozbawiony zostanie części funkcji (możliwość dokonywania zmian, możliwość przechowywania logów, etc.), które są realizowane przez system zarządzania. Równocześnie sytuacja taka nie ma miejsca jeżeli te wymagane funkcje są realizowane bezpośrednio przez komponent centralny. W związku z powyższym prosimy o informację, czy właściwym rozumieniem jest - celem uniknięcia opisanej sytuacji, a jednocześnie zachowania równoważności rozwiązań - iż należy przewidzieć w takiej sytuacji system zarządzania (komponent zarządczy) w konfiguracji analogicznej do komponentów centralnych tzn. urządzenia muszą być docelowo dostarczone w modelu redundantnym tzn. dwa urządzenia plus urządzenie cold spare. Jednocześnie taka konstrukcja komponentu zarządczego wydaje się być od strony niezawodnościowej

równoważna dla systemu zarządczego opartego o maszynę wirtualną, którego niezawodność i wysoka dostępność jest zapewniana przez hipernadzorcę KVM.

Odpowiedź:

Zamawiający w odpowiedzi na pytanie 1 z dnia 30/12/2021 stwierdził co następuje: „Zamawiający akceptuje rozwiązanie tego samego producenta, na którym logi i konfiguracja będą przechowywane w komponencie zarządczym, z zaoferowaną przez dostawcę przestrzenią dyskową działającą w RAID-1, RAID-5, RAID-6 lub RAID-10 pod warunkiem, że logi będą mogły być bezpośrednio i automatycznie przesyłane z komponentu zarządczego, z wykorzystaniem co najmniej protokołu SYSLOG, do zewnętrznego narzędzia składowania logów. W takim przypadku Zamawiający wymaga dodatkowo, aby przestrzeń przeznaczona na przechowywanie logów na komponencie zarządczym była co najmniej takiej samej wielkości, jakiej Zamawiający żąda na komponencie centralnym."

Zamawiający dopuścił to rozwiązanie aby nie ograniczać konkurencji. Wykonawca oferujący takie rozwiązanie oparte na urządzeniu fizycznym jest zobowiązany dostarczyć dwa takie fizyczne urządzenia zarządcze działające w modelu redundantnym.

Zamawiający wyjaśnia dodatkowo, że dopuszczone powyżej rozwiązanie dotyczy wyłącznie przeznaczonej na system operacyjny oraz dzienniki zdarzeń (logi) przestrzeni dyskowej niezbędnej do prawidłowego działania komponentu centralnego i nie dotyczy dodatkowo punktowanej dodatkowej przestrzeni dyskowej ponad wymagane 480GB. Zamawiający nie przyzna punktów za dodatkową przestrzeń dyskową ponad wymagane 480GB, która będzie zrealizowana na innym elemencie Systemu niż na komponencie centralnym.

Tym samym Zamawiający informuje, że w oparciu o art. 137 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2021 r., poz. 1129) zwaną dalej ustawą Pzp, dokonuje zmian treści Specyfikacji Warunków Zamówienia dalej SWZ przed upływem terminu składania ofert.

Dokonane zmiany treści SWZ Zamawiający udostępnia na stronie internetowej prowadzonego postępowania poprzez zamieszczenie ujednoliconej wersji SWZ z zaznaczonymi zmianami w pliku pod nazwą: SWZ_dostawa NGFW_zmiana_SWZ2.pdf

II.

Zamawiający informuje, że w dniu 12.01.2022 r. wpłynął wniosek o wyjaśnienie treści SWZ dotyczącej ww. postępowania o udzielenie zamówienia publicznego, na który Zamawiający zgodnie z art. 135 ust. 2 ustawy Pzp, udziela następujących wyjaśnień:

Pytanie 1.

W związku z publikacją odpowiedzi na pytania potencjalnych Wykonawców, w których Zamawiający doprecyzował wymagania techniczne, a wskutek czego zmienił w sposób istotny wymagania techniczne, czy zgodzi się na nieznaczne obniżenie wymagań przepustowości przy włączonej kontroli aplikacji do poziomu 64 Gbps oraz przepustowości przy włączonych co najmniej funkcjach kontroli aplikacji, IPS, AV do poziomu 17 Gbps. Wnosimy o zmianę, gdyż obecne zapisy parametrów technicznych oraz kryteria oceny ofert zawarte w SWZ jednoznacznie wskazują rozwiązania konkretnego producenta co ogranicza konkurencję oraz dają podstawy twierdzić, że Zamawiający wybiera konkretne rozwiązanie przed etapem złożenia ofert. Obecna sytuacja zmusza pozostałych potencjalnych Wykonawców do zaoferowania rozwiązań droższych co nie jest w interesie

Zamawiającego. Zaproponowana zmiana w bardzo małym stopniu wpłynie na parametry techniczne, natomiast znacząco poszerzy grono potencjalnych Wykonawców.

Odpowiedź:

Zamawiający wyraża zgodę na proponowaną zmianę parametrów.

Tym samym Zamawiający informuje, że w oparciu o art. 137 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2021 r., poz. 1129) zwaną dalej ustawą Pzp , dokonuje zmian treści Specyfikacji Warunków Zamówienia dalej SWZ przed upływem terminu składania ofert.

Dokonane zmiany treści SWZ Zamawiający udostępnia na stronie internetowej prowadzonego postępowania poprzez zamieszczenie ujednoliconej wersji SWZ z zaznaczonymi zmianami w pliku pod nazwą: SWZ_dostawa NGFW_zmiana_SWZ2.pdf

Pytanie 2.

Zamawiający wskazuje na możliwość otrzymania aż 20 dodatkowych punktów w postępowaniu dla oferty, która w ramach urządzenia głównego NGFW posiadać będzie funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, a następnie odszyfrowany ruch zostanie przekazany do zewnętrznych urządzeń bezpieczeństwa, które po analizie ten ruch zwrócą do NGFW. Według naszej najlepszej wiedzy tego typu funkcjonalność jest realizowana tylko na urządzeniach NGFW jednego producenta, Palo Alto Networks (https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-broker.html#id181JEB0K0U1), co sprawia, że osiągnięcie dodatkowych 20 punktów jest niemożliwe do uzyskania przez innych oferentów, tym samym zawężając możliwość konkurencyjności w niniejszym postępowaniu. Zwracamy się z prośbą o wycofanie dodatkowego punktowania za zrealizowanie deszyfracji SSL/TLS w opisanej powyżej formie na urządzeniu NGFW by wyrównać szanse wszystkich oferentów na udział w postępowaniu lub dodanie zapisów mówiących o przyznaniu dodatkowych punktów za zaoferowanie rozwiązań zewnętrznych, współpracujących z NGFW i działających z określoną wydajnością. Chcemy w tym momencie wskazać na zalety wykorzystania dedykowanego rozwiązania dla deszyfracji połączeń SSL/TLS. Zastosowanie dodatkowego rozwiązania w tym celu pozwoli zmniejszyć koszty projektu. Wsparcie deszyfracji SSL na urządzeniach NGFW powoduje znaczący spadek wydajności, sięgający w niektórych przypadkach nawet do 80% bazowej wydajności urządzenia, w zależności od poziomu skomplikowania wykorzystanych kluczy szyfrujących. Testy NSS Labs z roku 2019 wskazały, że dla ruchu szyfrowanego, uśredniona wydajność urządzenia ze wszystkich przeprowadzonych testów na dostępnych kluczach szyfrowania w testowanym rozwiązaniu Palo Alto Networks PA 5220 spowodowała degradację wydajności o co najmniej 50%, a w niektórych testach wartość ta dochodziła nawet do 97% (NSS Labs Next Generation Firewall Test Report – Palo Alto Networks PA-5220 PAN-OS 8.1.6-h2). Podobna sytuacja będzie występować na innych rozwiązaniach NGFW z uruchomioną dekrypcją SSL/TLS. Rozwiązania zewnętrzne, stosowane tylko w celu deszyfracji SSL/TLS, posiadają dedykowaną akcelerację sprzętową dla obsługi nawet najbardziej zaawansowanych kluczy szyfrowania i nie niosą ze sobą ryzyka obniżenia wydajności w przetwarzanym ruchu sieciowym, które w następstwie mogą skutkować powstawaniem wąskich gardeł w sieci i występowaniem znacznych opóźnień. Inną ważną zaletą jest skalowalność platform i elastyczność. Stosując odrębne urządzenia do realizowania ochrony w postaci NGFW oraz deszyfracji SSL można dużo lepiej dobrać odpowiadające potrzebom rozwiązania z zastosowaniem odpowiedniego bufora wydajności dla perspektywy zwiększenia ruchu w przyszłości, a także łatwiejszej wymiany na nowsze, bardziej wydajne

urządzenia, nie niosącej ze sobą konieczności inwestowania w duży appliance zawierający wszystkie te funkcjonalności w jednym systemie. Zastosowanie zewnętrznego rozwiązania pozwala również na dużo lepszy service chain, pozwalając na wszechstronną integrację kolejnych systemów za pomocą chociażby ICAP czy uruchamiając rozwiązanie jako TAP. Ostatnią korzyścią są wspominane już klucze szyfrowania. Ze względu na dedykowaną akcelerację sprzętową dla deszyfracji, rozwiązania zewnętrzne posiadają znacznie szerszą paletę możliwych do wykorzystania zestawów kluczy przy jednoczesnym utrzymaniu obecnej tendencji flow ruchu. W związku z powyższym, raz jeszcze zwracamy się z prośbą o niestosowanie dodatkowej punktacji za realizowanie funkcji SSL Offloading w ramach platformy NGFW lub przyznawanie punktów za zastosowanie rozwiązań zewnętrznych z określoną wydajnością pracy. Wnosimy o zmianę postanowień SWZ w taki sposób aby punktowane były tak samo rozwiązania spełniające wymagania wydajnościowe postawione przez Zamawiającego, ale składające się z komponentów zewnętrznych.

Odpowiedź:

Zamawiający nie wyraża zgody na proponowaną zmianę.

W postępowaniu mogą brać udział wykonawcy którzy nie oferują rozwiązania polegającego na deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach w urządzeniu głównym NGFW. Rozpoznanie rynku przeprowadzone przez Zamawiającego wskazuje, że rozwiązania polegające na deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach jest znacząco droższe od rozwiązań oferujących taką deszyfrację w oparciu o urządzenia zewnętrzne, zatem wykonawcy oferujący rozwiązanie w oparciu o urządzenia zewnętrzne mogą nie tylko wziąć udział w postepowaniu ale także ich oferta może być uznana za najkorzystniejszą po uwzględnieniu wszystkich kryteriów ocen ofert, w szczególności kryterium ceny.

III.

Zamawiający informuje, że w dniu 13.01.2022 r. wpłynął wniosek o wyjaśnienie treści SWZ dotyczącej ww. postępowania o udzielenie zamówienia publicznego, na który Zamawiający zgodnie z art. 135 ust. 2 ustawy Pzp, udziela następujących wyjaśnień:

Pytanie 1.

17. Komponent centralny musi posiadać funkcjonalność system wykrywania i zapobiegania włamaniom (Intrusion Prevention System – IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System musi działać w warstwie 7 modelu OSI. Baza sygnatur systemu wykrywania i zapobiegania włamaniom musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł systemu wykrywania i zapobiegania włamaniom musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji bez względu na numery portów, na których działa. Zamawiający wymaga dostarczenia licencji na system wykrywania i zapobiegania włamaniom w chwili dostarczenia urządzenia będącego komponentem centralnym. Okres trwania licencji musi być co najmniej taki sam jak okres gwarancji na urządzenie.

Wnosimy, aby Zamawiający zmienił zmodyfikowane w dniu 7 stycznia wymaganie poprzez zmianę użytego wyrażenia „aplikacji” na „usługo”. Tym samym wnosimy, aby wymaganie brzmiało:

Komponent centralny musi posiadać funkcjonalność system wykrywania i zapobiegania włamaniom (Intrusion Prevention System – IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System musi działać w warstwie 7 modelu OSI. Baza sygnatur systemu wykrywania i zapobiegania włamaniom musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł systemu wykrywania i zapobiegania włamaniom musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania **usługi** bez względu na numery portów, na których działa. Zamawiający wymaga dostarczenia licencji na system wykrywania i zapobiegania włamaniom w chwili dostarczenia urządzenia będącego komponentem centralnym. Okres trwania licencji musi być co najmniej taki sam jak okres gwarancji na urządzenie.

Odpowiedź:

Zamawiający wyjaśnia, że przez określenie „aplikacje" rozumie również różnie pojęte usługi (np. w konfiguracji klient-serwer) które są źródłem ruchu sieciowego.

Pytanie 2.

Komponent centralny musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak np. http, smtp, imap, pop3, ftp, smb itp. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent urządzenia na którym realizowana jest ta funkcja. Moduł AV musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania **aplikacji** bez względu na numery portów, na których działa. Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili dostarczenia urządzenia będącego komponentem centralnym. Okres trwania licencji musi być co najmniej taki sam jak okres gwarancji na urządzenie.

Wnosimy, aby Zamawiający zmienił zmodyfikowane w dniu 7 stycznia wymaganie poprzez zmianę użytego wyrażenia „aplikacji" na „usługi". Tym samym wnosimy, aby wymaganie brzmiało:

Komponent centralny musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak np. http, smtp, imap, pop3, ftp, smb itp. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent urządzenia na którym realizowana jest ta funkcja. Moduł AV musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania **usługi** bez względu na numery portów, na których działa. Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili dostarczenia urządzenia będącego komponentem centralnym. Okres trwania licencji musi być co najmniej taki sam jak okres gwarancji na urządzenie.

Odpowiedź:

Zamawiający wyjaśnia, że przez określenie „aplikacje" rozumie również różnie pojęte usługi (np. w konfiguracji klient-serwer) które są źródłem ruchu sieciowego.

IV.

Zamawiający w nawiązaniu do art. 137 ust. 6 ustawy Pzp wskazuje, iż wprowadzone zmiany treści SWZ są istotne dla sporządzenia ofert przez wykonawców oraz mogą wymagać od wykonawców dodatkowego czasu na zapoznanie się ze zmianą SWZ i przygotowanie ofert. Tym samym **Zamawiający informuje, że niżej wymienione terminy uległy zmianie:**

I. w Części I Część opisowa pkt. 13 w następujący sposób:

Było:

Wykonawca będzie związany ofertą przez okres 90 dni tj. **do dnia 16 kwietnia 2022 r**.
Bieg terminu związania ofertą rozpoczyna się wraz z upływem termin składania ofert.

Jest po zmianie:

Wykonawca będzie związany ofertą przez okres 90 dni tj. **do dnia 19 kwietnia 2022 r**.
Bieg terminu związania ofertą rozpoczyna się wraz z upływem termin składania ofert.

II. w Części I Część opisowa pkt. 15.1.1) w następujący sposób:

Było:

Ofertę wraz z wymaganymi dokumentami należy umieścić na platformie zakupowej pod adresem: https://platformazakupowa.pl/pn/pcss_poznan w myśl ustawy Pzp na stronie internetowej prowadzonego podstępowania do dnia **17 stycznia 2022 r. do godz. 11:00.**

Jest po zmianie:

Ofertę wraz z wymaganymi dokumentami należy umieścić na platformie zakupowej pod adresem: https://platformazakupowa.pl/pn/pcss_poznan w myśl ustawy Pzp na stronie internetowej prowadzonego podstępowania do dnia **20 stycznia 2022 r. do godz. 11:00.**

III. w Części I Część opisowa pkt. 15.2.1) w następujący sposób:

Było:

Otwarcie ofert nastąpi w dniu **17 stycznia 2022 r. o godz. 12:00** za pośrednictwem https://platformazakupowa.pl/pn/pcss_poznan.

Jest po zmianie:

Otwarcie ofert nastąpi w dniu **20 stycznia 2022 r. o godz. 12:00** za pośrednictwem https://platformazakupowa.pl/pn/pcss_poznan.

Z poważaniem,