L. Dz. 6/01/2022 Poznań, 4 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 21.12.2021 r. wpłynął wniosek o wyjaśnienie treści SWZ dotyczącej ww. postępowania o udzielenie zamówienia publicznego.

Pytanie 1.

Dokonywany przez Zamawiającego w Specyfikacji Istotnych Warunków Zamówienia(SIWZ) opis przedmiotu zamówienia wpływa na przebieg postępowania o udzielenie zamówienia publicznego oraz stanowi o istotnych postanowieniach późniejszej umowy. Stąd też, na Zamawiającym spoczywa obowiązek jasnego i precyzyjnego określenia przedmiotu zamówienia, a co za tym idzie, wykorzystania do jego opisania standardowych określeń technicznych, które są zwykle używane w danej dziedzinie, zrozumiałych dla wszystkich osób trudniących się działalnością w danej branży.

Art. 29 ust. 1 prawa zamówień publicznych nakłada na zamawiającego obowiązek opisania przedmiotu zamówienia w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględnienia wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty. Zapis ten służy realizacji ustawowych zasad uczciwej konkurencji a co za tym idzie zasady równego dostępu do zamówienia, wyrażonych art. 7 ust. 1 ustawy. Biorąc pod uwagę zapis art. 29 ust. 2 prawa zamówień publicznych, zgodnie, z którym przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, wystarczy do stwierdzenia faktu nieprawidłowości w opisie przedmiotu zamówienia, a tym samym sprzeczności z prawem, jedynie zaistnienie możliwości utrudniania uczciwej konkurencji poprzez zastosowanie określonych zapisów w specyfikacji, niekoniecznie zaś realnego uniemożliwienia takiej konkurencji. Zgodnie z wyrokiem Zespołu Arbitrów z dnia 18 grudnia 2003r. zamawiający powinien unikać wszelkich sformułowań lub parametrów, które by wskazywały na konkretny wyrób albo na konkretnego wykonawcę. Nie można mówić o zachowaniu zasady uczciwej konkurencji w sytuacji, gdy przedmiot zamówienia określony jest w sposób wskazujący na konkretny produkt, przy czym produkt ten nie musi być nazwany przez zamawiającego. Wystarczy, że wymogi i parametry dla przedmiotu zamówienia określone są tak, że aby je spełnić oferent musi dostarczyć jeden konkretny produkt.

Zamawiający wskazując w specyfikacji istotnych warunków zamówienia na konkretny produkt a pomijając minimalne wymagania dające obraz realnych oczekiwań, co do oferowanego produktu, nie tylko narusza zasadę określoną w art. 29 ust. 1 pkt. 3 ustawy, ale także zasadę uczciwej konkurencji i zasadę równego dostępu do zamówienia publicznego określone art. 7 ust. 1 prawa zamówień

publicznych, zniechęcając do udziału w postępowaniu wykonawców oferujących produkty innych marek.

Przepis art. 93 ust. 1 pkt. 7 prawa zamówień publicznych nakłada na zamawiającego obowiązek unieważnienia postępowania w sytuacji, gdy postępowanie obarczone jest wadą uniemożliwiającą zawarcie ważnej umowy w sprawie zamówienia publicznego. Z treścią tego przepisu koresponduje wyliczenie naruszeń postępowania skutkujące nieważnością umowy, dokonane art. 146 ust. 1 prawa zamówień publicznych, co pozwala na wskazanie m.in. przypadków, w których zachodzi bezwzględna konieczność unieważnienia postępowania. Wśród takich przypadków jest opisana art. 146 ust. 1 pkt. 6 prawa zamówień publicznych sytuacja, kiedy w postępowaniu o zamówienie publiczne doszło do naruszenia przepisów określonych w ustawie, a następnie naruszenie to miało wpływ na wynik postępowania, oraz sytuacja określona art. 146 ust. 1 pkt. 5, który odwołuje się do dokonania wyboru oferty z rażącym naruszeniem ustawy.

Zamawiający opisuje przedmiot zamówienia na tyle dokładnie, że wskazuje konkretny produkt, choć nie czyni tego expressis verbis.

Niewątpliwie takie postępowanie zamawiającego narusza zasady uczciwej konkurencji i zasadę równości. Do stwierdzenia faktu nieprawidłowości w opisie przedmiotu zamówienia, a tym samym sprzeczności z prawem, wystarczy jedynie zaistnienie możliwości utrudnienia uczciwej konkurencji poprzez posłużenie się określonymi zapisami w specyfikacji istotnych warunków zamówienia, niekoniecznie zaś realnego uniemożliwienia konkurencji. Wykonawca nie musi udowadniać, że określenia zawarte w dokumentacji związanej z postępowaniem, odnoszące się do przedmiotu zamówienia, faktycznie tę uczciwą konkurencję naruszają. Fakt naruszenia przez zamawiającego art. 7 ust. 1 i art. 29 ust. 2 Ustawy wymaga tylko uprawdopodobnienia (por. wyrok KIO z dnia 13 kwietnia 2010 r., KIO/UZP 440/10).

Potwierdzeniem powyższego jest m. in. wyrok Krajowej Izby Odwoławczej z dnia 7 czerwca 2010 r. (KIO/UZP 961/10), który dotyczy postępowania, w którym wykonawca zarzucił zamawiającemu opisanie przedmiotu zamówienia w sposób naruszający zasadę uczciwej konkurencji z uwagi na ograniczenie kręgu potencjalnych wykonawców do jednej firmy, dysponującej wymaganymi przez zamawiającego suszarkami typu taśmowego, gdzie przedmiotem zamówienia była budowa systemu termicznej przeróbki osadów. W przytoczonym orzeczeniu Krajowa Izba Odwoławcza stwierdziła, że nieistotnym jest argument podnoszony przez zamawiającego, iż przedmiotem zamówienia są roboty budowlane, a nie dostawa suszarek osadów, dlatego też nie można mówić o ograniczeniu konkurencji w zakresie robót budowlanych, ponieważ każdy z wykonawców robót budowlanych może zakupić w celu realizacji przedmiotu zamówienia odpowiednie, to znaczy spełniające wymagania SIWZ, urządzenia. W ocenie KIO, zamawiający dokonując opisu instalacji, która jest najważniejszym zespołem urządzeń mającym być zainstalowanym w trakcie realizacji przedmiotu zamówienia w sposób, który może preferować jednego z wielu producentów takich instalacji, utrudnia tym samym konkurencję wśród wszystkich wykonawców robót budowlanych.

Zgodnie z powyższym, zamawiający powinien w taki sposób sformułować przedmiot zamówienia, aby w żadnym aspekcie nie utrudniał uczciwej konkurencji, zarówno w sposób bezpośredni jak i pośredni, choćby przez narzucenie wykonawcy jakiegoś elementu składającego się na dostawę, usługę, czy robotę budowlaną. Powyższe stanowisko potwierdza również uchwała Krajowe Izby Odwoławczej z dnia 7 sierpnia 2009 r. (KIO/KD 20/09), w której wskazano, że opisanie zamówienia w sposób, który dyskryminuje jakikolwiek produkt stanowiący element składowy zamówienia bez uzasadnionej

przyczyny stoi w sprzeczności z zasadą równego dostępu do zamówienia i zasadą uczciwej konkurencji, wyrażoną odpowiednio w art. 7 ust. 1 i art. 29 ust. 2 Ustawy.
Niniejszym pragniemy poinformować, że według najlepszej naszej wiedzy jedynym rozwiązaniem spełniającym wymogi postępowania jest urządzenie PA-5450 z jedną kartą PA-5400-DPC-A którego producentem jest firma Palo Alto Networks.

Parametry urządzenia:

Table 1: PA-5450 Performance and Capacities		
	PA-5450 Configured System*	Single PA-5400-DPC-A
Firewall throughput (HTTP/appmix)***	200/200 Gbps	64.3/68 Gbps
Threat Prevention throughput (HTTP/appmix)†	120/148 Gbps	30.2/37 Gbps
IPsec VPN throughput‡	79 Gbps**	15.8 Gbps
Max sessions	100M**	20M
New sessions per second§	3.5M**	700,000
Virtual systems (base/max)‖	25/225	—

Wymagane karty:

Networking Cards

For network connectivity, the PA-5450 requires at least one NC (PA-5400-NC-A). A second NC requires a minimum of two DPCs installed in the system. A maximum of two NCs can be installed. NCs are dedicated to executing packet ingress and egress tasks.

Each PA-5400-NC-A offers multiple connectivity ports as listed in Table 3: 100/1000/10G Cu (4), 1G/10G SFP/SFP+ (12), and 40G/100G QSFP28 (2).

oraz dodatkowo punktowana powierzchnia dyskowa:

Storage Capacity
480 GB SSD, RAID1, system storage 4 TB SSD, log storage (optional)

W związku z powyższym zawracamy uwagę Zamawiającego, że w tym postępowaniu zostało naruszone prawo. W naszej ocenie, Zamawiającemu powinno zależeć na tym, aby umożliwić udział w postępowaniu większej liczbie uczestników, co jest korzystne dla Zamawiającego – chociażby poprzez uzyskanie niższej ceny, a co za tym idzie oszczędności budżetowe, co dla jednostki czerpiącej finansowanie z budżetu Państwa powinno stanowić priorytet.
W tym przypadku jedynym dostawcą, który został przez Zmawiającego dopuszczony jest firma Palo Alto Networks.

Jednocześnie informujemy, że zgodnie z przedstawionymi wyżej faktami, jako jeden z czołowych producentów rozwiązań bezpieczeństwa, co było wielokrotnie potwierdzane m.in.: w raportach firmy Gartner w obecnym stanie dokumentacji przetargowej nie jesteśmy w stanie złożyć oferty.

Odpowiedź:

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.

Dokonaną zmianę 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_SWZ1.pdf

II.

Zamawiający informuje, że w dniu 23.12.2021 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.

9. System musi umożliwiać automatyzację migracji/skopiowania konfiguracji z aktualnych urządzeń posiadanych przez zamawiającego (urządzenia te funkcjonują w oparciu o system JunOS w wersji 18 i wyższej dla SRX serii 5000) do dostarczanych urządzeń komponentu centralnego, bazując na tej samej składni i semantyce konfiguracji lub automatycznej konwersji konfiguracji/polityk bezpieczeństwa i obiektów bezpieczeństwa, do składni producenta Systemu dostarczonego przez wykonawcę, dostarczając narzędzie do konwersji wraz z wymaganą licencją na okres minimum jednego roku (o ile uzyskanie takiej licencji jest wymagane).

Wnosimy o dopuszczenie dostarczenia usługi migracji konfiguracji na koszt dostawcy.

Odpowiedź:

Zamawiający informuje, że nie dopuszcza możliwości dostarczenia usługi migracji konfiguracji na koszt dostawcy, z następujących powodów:

1. Konfiguracja wewnętrznych systemów bezpieczeństwa jest dla Zamawiającego kwestią poufną i krytyczną dla bezpieczeństwa organizacji. W związku z tym Zamawiający nie może udostępniać treści konfiguracji organizacji zewnętrznej (np. wykonawcy usługi migracji).
2. Dotychczasowa praktyka działania wskazuje, że proces zmiany konfiguracji jest działaniem wieloetapowym a co za tym idzie konieczne jest wielokrotne dokonywanie migracji także w odniesieniu do części konfiguracji. Z tych powodów Zamawiający nie jest w stanie określić z wyprzedzeniem ani liczby, ani terminów migracji. Zamawiający zaznacza przy tym, że procedura migracji odbywać się musi w sposób minimalizujący możliwość wystąpienia problemów w codziennej pracy organizacji. Wobec powyższego Zamawiający nie może:
   a) ponosić niemożliwych do określenia kosztów wielokrotnej realizacji usługi migracji;
   b) uzależnić się od zewnętrznego dostawcy usługi konfiguracji w zakresie możliwości świadczenia usługi w ogóle, a ponadto w trybie na żądanie oraz bez zbędnej zwłoki.

Pytanie 2.

2. Urządzenie NGFW będące komponentem centralnym musi być wyposażone w:

a. minimum 12 interfejsów o przepustowości minimum 10 Gbps (10 Gigabit Ethernet).

b. minimum 2 interfejsy o przepustowości minimum 100 Gbps (100 Gigabit Ethernet)

c. przestrzeń dyskową do przechowywania logów oraz nagrań ruchu o pojemności nie mniejszej niż 1TB (podane jako przestrzeń użyteczna) działająca w RAID-1.

Wnosimy o dopuszczenie urządzeń posiadających dysk o pojemności 480 GB. Zgodnie z dobrymi praktykami, logi oraz inne dane nie powinny być przechowywane lokalnie na urządzeniach,

a w dedykowanych systemach zarządzania urządzeniami. Wymaganie posiadania tak dużych dysków w urządzeniach NGFW jest nadmiarowe i służy jedynie ograniczeniu konkurencji.

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ1.pdf

Pytanie 3.

4. Komponent centralny musi spełniać co najmniej następujące parametry wydajnościowe:

a. • minimum 65 Gbps dla stanowego Firewall dla ruchu IPMIX/appmix,

b. • minimum 24 Gbps dla IPS dla ruchu IPMIX/appmix,

c. • minimum 600 tys. nowych połączeń na sekundę

d. • minimum 20 000 000 równoległych sesji.

Wnosimy o dopuszczenie urządzeń pozwalających nawiązywać minimum 435 tys. nowych połączeń na sekundę. Z dokumentacji Zamawiającego wynika, że wymaga on 1 000 tuneli IPSEC VPN (site-to-site), a co za tym idzie liczba 600 tys nowych połączeń wydaje się być nadmiarowe.

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ1.pdf

Pytanie 4.

10. Komponent centralny musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej:

a. oznaczania pakietów znacznikami DiffServ,

b. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego,

c. utworzenia co najmniej 8 klas ruchu sieciowego,

d. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

Wnosimy o wykreślenie punkty d. według najlepszej wiedzy Wykonawcy jest to funkcjonalność charakterystyczna tylko dla jednego producenta – firmy Palo Alto

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ1.pdf

Pytanie 5.

15. Polityka bezpieczeństwa komponentu centralnego musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe,

aplikacje, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Komponent centralny musi umożliwiać zdefiniowanie nie mniej niż 20 000 reguł polityki bezpieczeństwa oraz obsługę minimum 2000 stref bezpieczeństwa.
Prosimy o informację na jakiej podstawie Zamawiający wyliczył konieczność obsługi 2000 stref bezpieczeństwa. Czy wymaganie to oparte jest na posiadanej aktualnie infrastrukturze. Ile stref bezpieczeństwa w chwili obecnej jest obsługiwanych u Zamawiającego przez pracujące obecnie urządzenia NGFW.
Wnosimy jednocześnie o dopuszczenie urządzeń obsługujących 1000 stref bezpieczeństwa.
Odpowiedź:
Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.
Dokonaną zmianę 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_SWZ1.pdf

Pytanie 6.
16. Komponent centralny musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów. Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji komponentu centralnego numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Komponent centralny musi wykrywać predefiniowane aplikacje wspieranych przez producenta (np. Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu lub z wykorzystaniem komponentu zarządczego.
Wnosimy, aby Zamawiający dopuścił tworzenie definicji nowych aplikacji za pomocą zewnętrznego narzędzia dostarczanego przez producenta rozwiązań NGFW. Wygenerowane definicje aplikacji są następnie importowane z poziomu komponentu zarządczego.
Odpowiedź:
Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.
Dokonaną zmianę 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_SWZ1.pdf

Zamawiający dopuszcza stosowanie zewnętrznego narzędzia. Zastosowanie tego narzędzia nie może jednak powodować powstania po stronie Zamawiającego dodatkowych kosztów, np. dodatkowych opłat z tytułu licencji, nieuwzględnionej w cenie ofertowej, zaś ewentualne licencje niezbędne do zrealizowania takiego rozwiązania muszą spełniać wymogi przewidziane dla tych licencji w SWZ.

Pytanie 7.
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 uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja w modelu wykrywania lub zapobiegania uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Komponent centralny musi zapewniać możliwość ręcznego tworzenia sygnatur bezpośrednio na urządzeniu lub z użyciem komponentu zarządczego. 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.
Czy Zamawiający dopuszcza rozwiązanie w ramach którego moduł IPS/IDS aktywowany jest per urządzenie ale administrator ma pełną możliwość konfiguracji jaka część ruchu będzie podlegała inspekcji i w jaki zakresie? Zakres inspekcji IPS/IDS definiowany jest na poziomie dedykowanej warstwy polityki Threat Prevention. W ramach definicji reguł warstwy Threat Prevention administrator ma możliwość elastycznego przypinania różnych profili bezpieczeństwa określających zasadę działania modułu IPS/IDS (np. zestaw syngatur) do realizacji ochrony różnych zasobów jak np. host, sieć, usługa.
Odpowiedź:
Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.
Dokonaną zmianę 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_SWZ1.pdf

Zamawiający wymaga możliwości zdefiniowania odpowiedniej polityki w stosunku do ruchu sieciowego posiadającego konkretną charakterystykę (określone cechy), ale nie wymaga, aby charakterystyka ta (cechy) była/były opisane w pojedynczej regule.

Pytanie 8.
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 uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja w modelu wykrywania lub zapobiegania uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Komponent centralny musi zapewniać możliwość ręcznego tworzenia sygnatur bezpośrednio na urządzeniu lub z użyciem komponentu zarządczego. 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.
Czy Zamawiający dopuszcza rozwiązanie w którym dodawanie nowych sygnatur IPS realizowane jest z poziomu centralnej konsoli zarządzania poprzez import sygantur definiowanych w formacie SNORT?

Odpowiedź:
Zamawiający wyjaśnia, iż dopuszcza rozwiązanie, w którym dodawanie nowych sygnatur IPS realizowane jest z poziomu komponentu zarządczego poprzez import sygnatur definiowanych w formacie SNORT.

Pytanie 9.
18. 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 uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 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.
Czy Zamawiający dopuszcza rozwiązanie w ramach którego moduł AV aktywowany jest per urządzenie ale administrator ma pełną możliwość konfiguracji jaka część ruchu będzie podlegała inspekcji i w jaki zakresie? Zakres inspekcji AV definiowany jest na poziomie dedykowanej warstwy polityki Threat Prevention. W ramach definicji reguł warstwy Threat Prevention administrator ma możliwość elastycznego przypinania różnych profili bezpieczeństwa określających zasadę działania modułu AV do realizacji ochrony różnych zasobów jak np. host, sieć, usługa.

Odpowiedź:
Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.
Dokonaną zmianę 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_SWZ1.pdf

Zamawiający wymaga możliwości zdefiniowania odpowiedniej polityki w stosunku do ruchu sieciowego posiadającego konkretną charakterystykę (określone cechy), ale nie wymaga, aby charakterystyka ta (cechy) była/były opisane w pojedynczej regule.

Pytanie 10.
Komponent centralny musi zapewniać możliwość zapisania minimum 20 poprzednich wersji konfiguracji w pamięci wewnętrznej urządzenia. Komponent centralny musi mieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
Wnosimy o dopuszczenie rozwiązań, gdzie konfiguracja zapisywana jest ręcznie a nie automatycznie. Według najlepszej wiedzy Wykonawcy, jest to cecha charakterystyczna tylko dla jednego wykonawcy – firmy Palo Alto.

Odpowiedź:
Zamawiający informuje, iż nie dopuszcza urządzeń charakteryzujących się możliwością jedynie ręcznego zapisu konfiguracji. Z doświadczenia Zamawiającego wynika, że w sytuacji krytycznej (np. poważnej awarii) występuje potrzeba wprowadzenia dużej liczby zmian w konfiguracji w bardzo krótkim czasie, a w części przypadków - szybkiego wycofania jednej lub wielu wprowadzonych zmian. Z tej perspektywy konieczność ręcznego zapisywania konfiguracji po każdej zmianie wydłuża czas reakcji na sytuację wyjątkową i zwiększa możliwość popełnienia omyłki pod presją czasu, polegającej na braku zapisu konfiguracji lub wprowadzeniu konfiguracji niewłaściwej. Pożądana przez Zamawiającego funkcjonalność ułatwia pracę oraz przyśpiesza proces odtwarzania poprzednich wersji konfiguracji w razie takiej potrzeby.
Jednocześnie Zamawiający nie zgadza się ze stwierdzeniem, że wskazany przez Wykonawcę producent jest jedynym zdolnym do zaoferowania produktu spełniającego postawione wymaganie. Zamawiający korzysta obecnie z rozwiązania klasy NGFW innego producenta, które spełnia to wymaganie z zapasem – dając możliwość automatycznego zapisu do 50 konfiguracji oraz dodatkowo możliwość porównania wcześniej zapisanych automatycznie konfiguracji między sobą (wyświetlenia różnic w konfiguracjach), co w przypadku awarii jest kluczowe. Według najlepszej wiedzy Zamawiającego automatyczny zapis wersji konfiguracji po jej modyfikacji wspierają co najmniej rozwiązania producentów (w kolejności alfabetycznej): Fortinet, Juniper, Palo Alto.

Pytanie 11.
1. Komponent zarządczy może być dostarczony w postaci dedykowanego urządzenia z oprogramowaniem lub w postaci maszyny wirtualnej (virtual appliance) działającej pod Kontrolą hipernadzorcy KVM (zamawiający jest w posiadaniu infrastruktury bazującej na hipernadzorcy KVM).
4. Zamawiający dopuszcza możliwość zastąpienia WebGui przez komponent zarządczy będącym urządzeniem fizycznym (appliance), wyłącznie w momencie kiedy dostawca zapewni wszystkie niezbędne składniki do jego działania w trybie wysokiej dostępności HA (w celu wykluczenia pojedynczego punktu awarii) oraz rozwiązanie to będzie umożliwiało dostęp dla 10 osób jednocześnie (W przypadku konieczności łączenia się do komponentu zarządczego przez aplikację nie działającą na systemach operacyjnych z rodziny GNU/LINUX wykonawca musi dostarczyć licencję na system obsługujący te aplikację wraz z licencją i oprogramowaniem umożliwiającym pracę zdalną na tym systemie 8 administratorom, umożliwiając im równoległe zarządzanie komponentem centralnym), z możliwością niezależnej pracy. System zamienny dla WebGui musi posiadać wszystkie niezbędne licencje i komponenty dla wyżej wymienionej specyfiki, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc. Gwarancja i wsparcie na opisany komponent musi trwać cały okres gwarancyjny komponentu centralnego.
Czy Zamawiający wymaga dostarczenia komponentu zarządczego w postaci maszyny wirtualnej czy fizycznej ponieważ punkt 1 i 4 są wzajemnie wykluczające.
Odpowiedź:
Zamawiający wyjaśnia, iż wymaga, aby zarządzanie urządzeniem będącym komponentem centralnym odbywało się z linii poleceń (CLI) i graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW co zostało opisane w SWZ w rozdziale IV "Szczegółowe wymagania dotyczące przedmiotu zamówienia" w sekcji pt. "Specyfikacja komponentu centralnego", pkt. 20. W przypadku jednak, gdy dostawca

zaoferuje komponent zarządczy będącym urządzeniem fizycznym (appliance), a nie w postaci maszyny wirtualnej (virtual appliance) działającej pod kontrolą hipernadzorcy KVM, Zamawiający dopuszcza zastąpienie funkcji zarządzania poprzez graficzną konsolę Web GUI i dostępną przez przeglądarkę WWW wyłącznie w sytuacji, gdy Wykonawca spełni określone wymagania, które zostały przez Zamawiającego uszczegółowione w punkcie 4 sekcji pt. "Specyfikacja komponentu zarządczego" rozdziału IV SWZ. Oznacza to, że Zamawiający ze względu na łatwość obsługi preferuje interfejs Web GUI, ale Wykonawca ma możliwość zastąpienia funkcji Web GUI w przypadku braku możliwości jej realizacji przez dostarczony komponent zarządczy, jednak wyłącznie w momencie, gdy zapewni spełnienie ww. wymagań. Wymagania te chronią Zamawiającego przed obniżeniem efektywności pracy oraz poniesieniem dodatkowych kosztów w sytuacji, w której Wykonawca nie jest w stanie dostarczyć preferowanego interfejsu Web GUI.

III.

Zamawiający informuje, że w dniu 27.12.2021 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 punkcie IV. Zamawiający opisał m.in. Specyfikację komponentu zapasowego Cold-Spare.
W szczególności Zamawiający wskazał, iż Komponent zapasowy cold-spare musi mieć możliwość przeniesienia licencji z uszkodzonych urządzeń centralnych lub jeżeli to nie możliwe, wymagane jest dostarczenie osobnych odpowiadających licencji dających możliwość odtworzenia klastra komponentów centralnych przy użyciu komponentu zapasowego „cold spare”
W naszej ocenie jest to wymaganie zasadne w przypadku, gdy oferowane urządzenia będą miały konstrukcję „zamkniętą” w rozumieniu takim, iż urządzenie będzie funkcjonowało jako niemodularne/nierozłączne. Wówczas każda awaria (poza zasilaczami) wymusza zastąpienie urządzenia produkcyjnego które uległo awarii urządzeniem w całości nowym i przeniesienia na nie licencji z urządzenia dotychczas określanego jako produkcyjne.
Jednocześnie pragniemy wskazać, iż w przypadku urządzeń modularnych uszkodzenie pojedynczego lub nawet kilku komponentów (karta zarządzania, karta interfejsów, etc) nie musi powodować wymiany urządzenia na nowe, a jedynie wymianę tych elementów które są niesprawne.
Stąd też prosimy o potwierdzenie, iż Zamawiający uzna ofertę za spełniającą wymagania, jeżeli jako komponent centralny zaoferowane zostanie urządzenie modularne oraz komponenty zapasowe stanowiące cold-spare i jednocześnie Zamawiający będzie wymagał przeniesienia licencji tylko w sytuacji gdy wymianie będzie ulegał moduł zarządzania (lub inny element urządzenia modularnego), do którego przypisane są same licencje.

Odpowiedź:

Zamawiający informuje, że ze względu na newralgiczny charakter przedmiotu zamówienia dla jego działalności nie dopuszcza zastąpienia urządzenia cold spare dostawą - na bliżej nieokreślonych warunkach - komponentów dodatkowych. Zamawiający w sytuacji wystąpienia awarii byłby uzależniony od wykonawcy usługi zewnętrznej (dostawcy i integratora elementów „zapasowych”). Zamawiający wymaga dostarczenia kompletnego urządzenia jako cold spare.

Pytanie 2

W punkcie IV. Zamawiający opisał m.in. Specyfikację komponentu centralnego.

W punkcie 4 Zamawiający określił iż wymaga wydajności minimum 65 Gbps dla stanowego Firewall dla ruchu IPMIX/appmix.

Z racji tego, że IPMIX odnosi się do kontroli ruchu L3/L4 ISO/OSI podczas gdy kontrola ruchu z wykorzystaniem aplikacji jako atrybutu odnosi się do wartswy L7 ISO/OSI prosimy o jednoznaczne potwierdzenie że Zamawiający wymaga dostawy urządzeń, które zapewniają wydajność 65Gbps dla stanowego firewall działającego w warstwie 7.

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ1.pdf

Pytanie 3

W punkcie IV. Zamawiający opisał m.in. Specyfikację komponentu centralnego.

W punkcie 2 Zamawiający określił iż wymaga by dostarczone urządzenie zapewniało przestrzeń dyskową do przechowywania logów oraz nagrań ruchu o pojemności nie mniejszej niż 1TB (podane jako przestrzeń użyteczna) działająca w RAID-1.

Jednocześnie w wymaganiach w p. 30 Zamawiający wskazuje wymaganie dodatkowo punktowane, gdzie „Komponent centralny może być wyposażony w dysk twardy do przechowywania logów i raportów o pojemności nie mniejszej niż 4 TB” przy czym nie określa już czy jest to przestrzeń użyteczna (działająca np. w RAID-1) czy całkowita.

W związku z powyższym prosimy o ujednolicenie wymagań i wskazanie czy przestrzeń 4TB należy rozumieć analogicznie jak w p.2 czyli podana jako przestrzeń użyteczna działająca w RAID-1 lub o wyjaśnienie wymagań.

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ1.pdf

Pytanie 4

W kilku miejscach specyfikacji Zamawiający wskazuje jednoznacznie, iż należy dostarczyć przedmiot umowy w terminie nie późniejszym niż 08 kwietnia 2022. Realnie jednak konieczne jest dostarczenie urządzeń kilka dni wcześniej.

Jednocześnie Zamawiający oczekuje związania Wykonawcy ofertą do dnia 09 kwietnia 2022 roku.

Może to spowodować sytuację, w której Zamawiający na podstawie tak sformułowanej Specyfikacji Warunków Zamówienia – w sposób nie zawiniony przez żadną ze stron, a wynikły np. z przebiegu postępowania przetargowego - będzie oczekiwał podpisania umowy w takim terminie (np. po

4 kwietnia 2022), gdy dostarczenie przedmiotu Zamówienia, jego odbiór oraz przesłanie odpowiednich dokumentów będzie po prostu nierealne.
Należy także zaznaczyć tutaj, iż urządzenia, których wymaga Zamawiający są zazwyczaj produkowane „pod zamówienie", a tym samym nie są przechowywane przez producentów w magazynach. Pragniemy też podkreślić, że w ostatnich miesiącach czasy dostaw wielu producentów wydłużyły się do kilkunastu tygodni i dostarczenie urządzeń w czasie 6-7 tygodni (jak jest to określone w etapie II) jest już samo w sobie dużym wyzwaniem dla dominującej części producentów.
Dlatego też wnosimy o zmianę wymagań dotyczących etapu 1 analogicznie do tych z etapu 2 – to znaczy, iż dostawa urządzeń będzie zrealizowana do 08 kwietnia 2022 z zastrzeżeniem, iż Wykonawca będzie miał minimum 60 dni na dostawę od dnia podpisania umowy,
Alternatywnie wnosimy o zmianę wymagań w taki sposób, że Wykonawca będzie mógł określić w ofercie realny czas dostawy, a jeżeli będzie on krótszy na dzień podpisywania umowy, wówczas Wykonawca będzie zobowiązany do potwierdzenia realizacji lub będzie miał możliwość odstąpienia od podpisania umowy.

Odpowiedź:

Zamawiający akceptuje propozycję Wykonawcy w zakresie dokonania zmiany wymagań dotyczących terminu dostarczenia przedmiotu zamówienia dotyczących etapu 1. Tym samym w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.
Dokonaną zmianę 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_SWZ1.pdf

Pytanie 5

W dokumencie II. Formularz Oferty Zamawiający zastrzega, iż cena za realizację etapu 1 nie może przekraczać 60% łącznej wartości sumarycznej wynagrodzenia za etap I i etap II.
Ze względu na fakt, iż część producentów nie zapewnia urządzeń cold-spare należy oczekiwać, że Zamawiający otrzyma oferty zawierające trzy jednakowe urządzenia. Tym samym cena każdego z nich będzie stanowić 33,3% ceny całkowitej.
Zastrzeżenie Zamawiającego powoduje, iż Wykonawcy będą zmuszenie zaoferować dwa z trzech urządzeń w cenie o 10% niższej od ich wartości (w przypadku gdy Zamawiający nie skorzysta z opcji zakupu trzeciego urządzenia). Biorąc pod uwagę powyższe wnosimy o zmianę wymagania w taki sposób, iż „cena za realizację etapu 1 nie może przekraczać 67% łącznej wartości sumarycznej wynagrodzenia za etap I i etap II.

Odpowiedź:

Zamawiający akceptuje propozycję Wykonawcy w zakresie dokonania zmiany wymagania w taki sposób, iż „cena za realizację etapu 1 nie może przekraczać 67% łącznej wartości sumarycznej wynagrodzenia za etap I i etap II. Tym samym w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.
Dokonaną zmianę 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_SWZ1.pdf

IV.

Zamawiający informuje, że w dniu 30.12.2021 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

1.Wymaganie:

2. Urządzenie NGFW będące komponentem centralnym musi być wyposażone w: ….

• przestrzeń dyskową do przechowywania logów oraz nagrań ruchu o pojemności nie mniejszej niż 1TB (podane jako przestrzeń użyteczna) działająca w RAID-1.

Pytanie:

Czy zamawiający zaakceptuje rozwiązanie tego samego producenta, na którym logi i konfiguracja będzie przechowywana w systemie Centralnego Zarządzania, z pojemnością dysku 4 TB w RAID 5? Konfiguracja ta zapewni zamawiającemu większą redundancję, poza tym odseparuje dane, zwiększa odporność na awarię pojedynczego punktu i umożliwia przechowywanie kopii zapasowych.

Odpowiedź:

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.

Pytanie 2

2. Wymaganie:

4. Komponent centralny musi spełniać co najmniej następujące parametry wydajnościowe: ..

- minimum 65 Gbps dla stanowego Firewall dla ruchu IPMIX/appmix,

Pytanie:

Podany model testowania Firewall Stanowego, jest wprost przepisany z karty dla rozwiązań producenta Palo Alto co znacząco ogarnicza konkurencyjność oferowanych rozwiązań. W celu umożliwienia dobrania odpowiedniej wydajności urządzenia proszę o podanie szczegółowych parametrów na podstawie których przyjęta została przepustowość rozwiązania. Czy zamawiający uwzględni za spełnione jeżeli rozwiązanie będzie miało przyjęty ruch IMIX tzw. internet MIX, który jest standardem w większości rozwiązań bezpieczeństwa?

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ.pdf

Pytanie 3

3. Wymaganie:

13. Komponent centralny musi obsługiwać nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do co najmniej 20 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:

Pytanie:

Czy zamawiający wymaga dostarczenie licencji na 10 wirtualnych firewalli/systemów/domen/kontekstów, czy zaś tylko wymaga posiadania takiej funkcjonalności?

Odpowiedź:

Zamawiający w oparciu o art. 137 ust. 1 ustawy Pzp, dokonuje zmian treści SWZ przed upływem terminu składania ofert.

Dokonaną zmianę 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_SWZ1.pdf

Pytanie 4

4. Wymaganie:

24. Komponent centralny musi zapewniać możliwość zapisania minimum 20 poprzednich wersji konfiguracji w pamięci wewnętrznej urządzenia. Komponent centralny musi mieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany

Pytanie :

Wymaganie przechowywania 20 ostatnich wersji konfiguracji jest typowe dla rozwiązań producenta Palo Alto co znacząco ogranicza konkurencyjność oferowanych rozwiązań. Czy zamawiający zaakceptuje rozwiązanie, które przechowuje 10 ostatnich wersji w pamięci wewnętrznej urządzenia zaś pozostałe konfiguracje będą mogły być przechowywane na zewnętrznej kopii zapasowej w infrastrukturze zamawiającego?

Odpowiedź:

Zamawiający nie wyraża zgody na proponowaną zmianę i wskazuje, że według jego najlepszej wiedzy kwestionowane wymaganie, dotyczące przechowywania minimum 20 ostatnich wersji konfiguracji spełniają urządzenia co najmniej 3 różnych producentów systemów klasy NGFW, takich jak (w kolejności alfabetycznej): Fortinet, Juniper, Palo Alto. Zamawiający korzysta obecnie z rozwiązania, które zapewnia automatyczny zapis oraz przechowywanie 50 ostatnich wersji konfiguracji i na podstawie codziennej praktyki uważa liczbę 10 ostatnich konfiguracji przechowywanych w pamięci wewnętrznej urządzenia za zbyt niską.

Pytanie 5

5. Wymaganie:

27. Komponent centralny posiada funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS. Odszyfrowany ruch zostaje przekazany do zewnętrznych urządzeń bezpieczeństwa, które po przeprowadzeniu analizy zwrócą ruch do komponentu centralnego, w celu jego dalszego

przetwarzania. Komponent centralny musi przy tym współpracować z zewnętrznymi urządzeniami bezpieczeństwa funkcjonującymi w trybie transparentnym lub w trybie L3 (funkcjonalność nazywana dalej inspekcją SSL/TLS).
Pytanie:
Czy zamawiający zaakceptuje rozwiązanie, w którym deszyfrowany ruch przesyłany jest jako kopia (mirror ruchu) przez dowolny wybrany interfejs na urządzeniu centralnym do docelowego analizatora ruchu?
Proszę o podanie listy zewnętrznych urządzeń bezpieczeństwa, z którymi powinien współpracować komponent centralny.
Odpowiedź:
Zamawiający nie dopuszcza rozwiązania, w którym deszyfrowany ruch przesyłany jest jako kopia (mirror ruchu) przez dowolny wybrany interfejs na urządzeniu centralnym do docelowego analizatora ruchu. W ocenie Zamawianego przesyłanie obrazu ruchu do zewnętrznego analizatora zwiększa ryzyko wystąpienia awarii.
Zamawiający zamierza wykorzystać co najmniej poniższe zewnętrzne narzędzia bezpieczeństwa:

- Suricata
- Zeek
- narzędzia klasy WAF

Pytanie 6
6. Wymaganie dodatkowo punktowane:
30. (Dodatkowo punktowane)
Komponent centralny może być wyposażony w dysk twardy do przechowywania logów i raportów o pojemności nie mniejszej niż 4 TB.
Pytanie:
Czy zamawiający zaakceptuje rozwiązanie tego samego producenta, na którym logi i konfiguracja będzie przechowywana i przetwarzania w systemie Centralnego Zarządzania, z pojemnością dysku 4 TB w RAID 5? Urządzenia centralne nadal będę przechowywać logi i konfigurację lecz do poziomu ograniczenia wielkością dysku
Odpowiedź:
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.

Pytanie 7
7. Wymaganie dodatkowo punktowane:
28. **[Dodatkowo punktowane]** System pozwala na import reguł zgodnych z rozwiązaniami SNORT i/lub Suricata do modułów systemu wykrywania i zapobiegania włamaniom komponentu centralnego.
Pytanie:

Czy zamawiający zaakceptuje rozwiązanie, w którym import reguł SNORT/ Suricata będzie poprzedzony konwersją na format sygnatur wspieranych przez oferowane rozwiązanie dydedykowanym narzędziem lub wsparciem prodcuenta?

Odpowiedź:

Zamawiający dopuszcza rozwiązanie, w którym import reguł SNORT/ Suricata będzie poprzedzony konwersją na format sygnatur wspieranych przez oferowane rozwiązanie za pomocą dedykowanego narzędzia producenta. Zastosowanie takiego rozwiązania nie może powodować obciążenia Zamawiającego jakimikolwiek dodatkowymi kosztami w terminie późniejszym (np. dodatkowymi opłatami licencyjnymi). Dostarczone oprogramowanie albo wsparcie musi obejmować licencję, zapewniającą możliwość użytkowania i (w przypadku oprogramowania) aktualizacji przez czas nieograniczony, bez możliwości wypowiedzenia licencji oraz bez jakikolwiek ograniczeń innego rodzaju (np. terytorialnych).

V.

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 9 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 16 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 **10 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 **17 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 **10 stycznia 2022 r. o godz. 12:00** za pośrednictwem https://platformazakupowa.pl/pn/pcss_poznan.

Jest po zmianie:

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

Z poważaniem,