Gorzów Wlkp. 05.03.2019r.

WAD-VI.271.23.2019.IKP

Wykonawcy biorący udział w postępowaniu

Dotyczy postępowania o udzielenie zamówienia publicznego pn. „ **Zakup przełączników dostępowych oraz systemu zabezpieczeń Firewall wraz z rozwiązaniem do bezpiecznej transmisji VPN**

Uprzejmie informuję, iż do Zamawiającego wpłynęły zapytania dotyczące przedmiotowego postępowania, na które udziela się następujących odpowiedzi:

Pytanie nr 1: ***dotyczy wymagania IV.3. B Opisu przedmiotu zamówienia***
*„System zabezpieczeń firewall musi być wyposażony w co najmniej … **4 port4** 1Gbps/**10Gbps** SFP/SFP+"*
W punkcie 2 Zamawiający wymaga urządzenia które posiada co najmniej 8 portów działających z prędkością 10Gb/s. Jednocześnie w punkcie 2 tego rozdziału Zamawiający pisze: *„System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 5000 **Mbit/s** dla kontroli firewall z włączoną funkcją kontroli aplikacji…"*
Da się zauważyć, że Zamawiający oczekuje urządzenia dla którego wydajność całego urządzenia jest mniejsza niż wydajność nawet jednego portu z czterech wymaganych przez Zamawiającego.
Analizując wymaganie, doszliśmy do wniosku, iż wymaganie *„12 portów Ethernet 10/100/1000, 4 porty Ethernet 1GbE SFP, 4 porty 1Gbps/10Gbps SFP/SFP+"* zostało najprawdopodobniej skopiowane z karty katalogowej urządzenia PA3220 producenta PaloAlto Networks, gdyż dokładnie taką ilość portów posiada to urządzenie.
Mając na uwadze powyższe, domniemamy, iż wymaganie to nie jest podyktowane rzeczywistą potrzebą Zamawiającego, a jedynie Zamawiający posłużył się kartą katalogową przy przygotowaniu opisu warunków zamówienia.
Prosimy zatem o dostosowanie wymagania do rzeczywistej potrzeby Zamawiającego i zmianę treści wymagania na *„System zabezpieczeń firewall musi być wyposażony w co najmniej 10 portów Ethernet 10/100/1000, **2 portów** 1Gbps/**10Gbps** SFP/SFP+"*

Jeżeli Zmawiający posiada rzeczywistą potrzebę wykorzystania **4 portów** 1Gbps/**10Gbps** SFP/SFP na urządzeniu NGFW, prosimy zatem o odpowiednie dostosowanie wymagań wydajnościowych do wymaganych 4 portów 10Gb/s i zmianę treści punktu 2 na brzmiącą:

„System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż **35000 Mbit/s** dla kontroli firewall , nie mniej niż 10000 Mbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 4000 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering), obsługiwać nie mniej niż 1 000 000 jednoczesnych połączeń, oraz zapewnić wydajność nie mniejszą niż 2500 Mbit/s dla ruchu szyfrowanego IPSec."

Odpowiedź : ***Zamawiający sprecyzował w SIWZ minimalne wymagania dotyczące interfejsów dla urządzenia stanowiącego przedmiot przetargu. Zamawiający określił te wymagania w sposób przejrzysty i nie wymagający dodatkowych wyjaśnień. Wymagania na liczbę portów 1Gbps/10Gbps SFP/SFP+ wynikają ze szczegółów budowy infrastruktury sieciowej Zamawiającego. Zamawiający podtrzymuje zapisy SIWZ.***

Pytanie nr 2: ***dotyczy wymagania IV.22 Opisu przedmiotu zamówienia***
Pragniemy zauważyć, że podany w tym wymaganiu zestaw typów plików w stu procentach jest obsługiwany tylko przez urządzenia producenta PaloAlto, a pozostali producenci rozwiązań będą posiadać jeden lub kilka typów nieobsługiwanych, co sprowadza się do sytuacji, iż w postępowaniu będzie można zaoferować rozwiązanie tylko jednego producenta.

Dodatkowo, jest to zestaw typów plików który jest skopiowany z karty katalogowej producenta PaloAlto i wiele z opisanych typów plików nie będą używane przez Zamawiającego gdyż są to pliki dedykowanego oprogramowania lub są przestarzałe, wycofane z użycia i zastąpione nowszymi typami. Przykładem takich typów plików są pliki typu mdi, pif, pgp, tif i inne...

Faworyzowanie jednego producenta jest niezgodne z ustawą o zamówieniach publicznych. W celu umożliwienia złożenia oferty dla rozwiązań innych niż tylko rozwiązanie PaloAlto Networks, prosimy o usunięcie opisów typów plików mało wykorzystywanych przez modyfikację wymagania na brzmiące: *System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, rar, zip, exe, gzip, hta, , pdf, pgp, tar, text/html, tif, pliki microsoft office, pliki zaszyfrowane. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.*

Odpowiedź : ***Zamawiający zmienia brzmienie wymagania na:***
"System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, rar, zip, exe, gzip, hta, , pdf, pgp, tar, text/html, tif, pliki microsoft office, pliki zaszyfrowane. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia."

Pytanie nr 3: ***dotyczy wymagania IV.24 Opisu przedmiotu zamówienia***
Pragniemy zwrócić uwagę, że rozwiązanie pozwalające na kontynuowanie transmisji zainfekowanego pliku niesie potencjalne zagrożenie i jest niezgodne z ogólnie przyjętymi najlepszymi praktykami przyjętymi w branży. Jak wiadomo, pod każdym względem systemy bezpieczeństwa dążą do automatyzacji i w tym właśnie celu instalowane są systemy NGFW by w trybie automatycznym reagować na zagrożenia i blokować transmisję zainfekowanych/niedozwolonych plików. Oddelegowanie do użytkownika końcowego decyzji o pobraniu niedozwolonego pliku z punktu widzenia bezpieczeństwa należy traktować w sposób, jak by w sieci zupełnie nie było zainstalowanego systemu NGFW i infrastruktura nie była chroniona. Właśnie dla tego funkcjonalność taka nie jest implementowana na rozwiązaniach bezpieczeństwa większości producentów.

Również Zamawiający rozumiejąc zasadność stosowania systemów NGFW w punkcie IV.13 wymaga aby, system zabezpieczeń działał zgodnie z zasadą „The Principle of Last Privilage" tzn, system zabezpieczeń powinien blokować wszystkie aplikacje, poza tymi, które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

Prosimy zatem o usunięcie wymagania **IV.24** gdyż jest ono **sprzeczne z** wymaganiem **IV.13** oraz funkcjonalność jest z zasady niezgodna i sprzeczna z ideą i najlepszymi praktykami wykorzystania systemów NGFW, które są tematem dzisiejszego postępowania. Również wymaganie to w połączeniu z pozostałymi wskazuje jednoznacznie na urządzenia producenta Palo Alto Networks.

Odpowiedź : ***Zamawiający przyjmuje argumentację Oferenta i zmienia brzmienie wymagania. Nowe brzemiennie wymagania: System zabezpieczeń firewall musi zapewniać ochronę przed atakami typy "drive-by-download".***

Pytanie nr 4 : ***dotyczy wymagania IV. „Wymagania podstawowe identyfikacji użytkowników" Opisu przedmiotu zamówienia***

Proszę o sprecyzowanie, dla których systemów innych niż MS Windows będzie wymagane będzie analizowanie informacji Syslog w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Proszę o podanie wersji systemów ich ilości oraz ilości

użytkowników korzystających z tych systemów. Informacja ta jest wymagana by Oferent mógł w precyzyjny sposób zwymiarować oferowane rozwiązanie.

Jeżeli na obecnym etapie nie jest możliwe określenie wymaganych informacji, prosimy o dopuszczenie rozwiązania które na etapie dostarczenia nie będzie posiadało uruchomionej wymaganej funkcjonalności lecz będzie posiadało możliwością rozbudowy o tą funkcjonalność z przyszłości.

Odpowiedź : ***Zamawiający sprecyzował w SIWZ minimalne wymagania dotyczące identyfikacji użytkowników dla urządzenia stanowiącego przedmiot przetargu. Zamawiający określił te wymagania w sposób przejrzysty. Biorąc pod uwagę przyszłe plany związane z rozbudową sieci miejskiej, Zamawiający nie dookreśla liczby użytkowników, jak też wersji systemów ze względu na ich różnorodność w poszczególnych jednostkach podległych. Zamawiający pragnie uzyskać możliwie elastyczne rozwiązanie, które będzie w stanie zaadresować różne scenariusze wdrożeniowe w sieci miejskiej. Ponadto, zgodnie z najlepszą wiedzą Zamawiającego, informacje, których żąda oferent nie są niezbędne, aby mógł w precyzyjny sposób zwymiarować urządzenie stanowiące przedmiot przetargu. Zamawiający podtrzymuje zapisy SIWZ.***

Pytanie nr 5 : ***dotyczy Opisu przedmiotu zamówienia wymagania IV. „Wymagania podstawowe identyfikacji użytkowników"***

Czy Zamawiający zaakceptuje rozwiązanie w którym funkcjonalność ta będzie realizowana w wykorzystaniem oddzielnej wchodzącej w skład systemu zabezpieczeń maszyny wirtualnej tego samego producenta i natywnie współpracującej z systemem firewall?

Odpowiedź : ***Zamawiający dopuszcza rozwiązanie, w którym funkcjonalność ta będzie realizowana w wykorzystaniem oddzielnych wchodzących w skład systemu zabezpieczeń maszyn fizycznych tego samego producenta i natywnie współpracujących z systemem firewall pod następującymi warunkami:***
Ze względu na to, iż Zamawiający nie posiada zwirtualizowanych zasobów obliczeniowych umożliwiających instalację i uruchomienie maszyn wirtualnych, Oferent dostarczy rozwiązanie wykorzystujące fizyczne urządzenia spełniające następujące wymagania:
- będzie wyprodukowane przez tego samego producenta co producent oferowanego Firewalla
- będzie objęte kontraktem serwisowym Producenta o tym samym okresie trwania, co kontrakty serwisowe oferowanych Firewalli
- będzie wyposażone w redundantne zasilacze
Podobnie jak urządzenia firewall dodatkowy system wspierający identyfikację użytkowników musi być dostarczony jako redundanta para urządzeń fizycznych.

Pytanie 6 : ***Dotyczy Opisu przedmiotu zamówienia IV. „Wymagania podstawowe identyfikacji użytkowników" pkt. 3***

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 (tak jest to realizowane przez większość topowych producentów NGFW).

Odpowiedź : ***Zamawiający zgadza się uprościć zapis, gdzie wystarczającym będzie rozpoznawanie adresów z nagłówków XFF, a uwierzytelnianie użytkownika dopuszczalne będzie per sesja.***

Pytanie nr 7 : ***Dotyczy Opisu przedmiotu zamówienia IV. „Wymagania ochrony IPS,AV, anty-spyware, URL, zero-day" pkt. 10***
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. Takie wyodrębnienie funkcjonalności/modułu

AntySpyware od AntyVirus występuje tylko w rozwiązaniu producenta PaloAlto Networks. Pozostali producenci ochronę AntySpyware wykonują w module/funkcjonalności AntyVirus lub IPS, bez widocznego ich dzielenia. Co więcej taka architektura rozwiązania pozwala na korzystniejsze zarządzanie .
Wymaganie to więc w jednoznaczny sposób faworyzuje rozwiązanie PaloAlto Networks, i blokuje możliwość zaoferowania innych konkurencyjnych i wielu przypadkach lepszych rozwiązań, co jest niezgodne z ustawą i postępowaniach publicznych.
Rozumiemy, iż intencją Zamawiającego jest skuteczna ochrona przed atakami typu Spyware, a nie jedynie zakup rozwiązania PaloAlto. Intencją Oferenta jest zaoferowanie wiodącego systemu bezpieczeństwa NGFW innego niż rozwiązanie Palo Alto Networks, posiadającego wiele niezależnych certyfikacji i rekomendacji, w tym posiadającego funkcjonalność AntySpyware zintegrowaną z funkcjonalnością AntyVirus. Prosimy zatem o usunięcie wymagania lub jednoznaczne potwierdzenie iż Zamawiający dopuszcza rozwiązania w których moduł/funkcjonalność AntySpyware jest częścią modułu/funkcjonalności AntyVirus, a baza sygnatur AntyVirus zawiera sygnatury AntySpyware.

Odpowiedź : ***Zamawiający sprecyzował w SIWZ minimalne wymagania dla urządzenia stanowiącego przedmiot przetargu. Zamawiający określił te wymagania w sposób przejrzysty i nie wymagający dodatkowych wyjaśnień. Żądanie ich usunięcia nie spowoduje zwiększenia konkurencyjności, gdyż praktycznie wszyscy liczący się producenci posiadają urządzenia o funkcjonalności spełniającej wymagania Zamawiającego.***

Wymagania dotyczące silnika i sygnatur anty-spyware są wymaganiami funkcjonalnymi – i tutaj Zamawiający posłużył się ogólnie przyjętą taksonomią. Jednocześnie w innych wymaganiach SIWZ Zamawiający dopuścił, aby ta funkcjonalność była realizowana w innych modułach funkcjonalnych (np. anty-malware jako moduł obejmujący anty-spyware). Zamawiający dopuszcza rozwiązania, w których moduł/funkcjonalność Anty-Spyware jest częścią moduły/funkcjonalności Anty-Virus, a baza sygnatur Anty-Virus zawiera sygnatury Anty-Spyware.

Pytanie nr 8 : ***Dotyczy Opisu przedmiotu zamówienia IV „Wymagania ochrony IPS,AV, anty-spyware, URL, zero-day" pkt. 11***

W nawiązaniu do pytania poprzedniego, prosimy o potwierdzenie iż iż Zamawiający dopuszcza rozwiązania w których moduł/funkcjonalność AntySpyware jest częścią modułu/funkcjonalności AntyVirus i wymaganie będzie spełnione jeżeli moduł/funkcjonalność AntyVirus będzie uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł/funkcja AntyVirus który prowadzi również inspekcję AntySpyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

Odpowiedź : ***Zamawiający sprecyzował w SIWZ minimalne wymagania dla urządzenia stanowiącego przedmiot przetargu. Zamawiający określił te wymagania w sposób przejrzysty i nie wymagający dodatkowych wyjaśnień. Żądanie ich usunięcia nie spowoduje zwiększenia konkurencyjności, gdyż praktycznie wszyscy liczący się producenci posiadają urządzenia o funkcjonalności spełniającej wymagania Zamawiającego.***

Wymagania dotyczące silnika i sygnatur anty-spyware są wymaganiami funkcjonalnymi – i tutaj Zamawiający posłużył się ogólnie przyjętą taksonomią. Jednocześnie w innych wymaganiach SIWZ Zamawiający dopuścił aby ta funkcjonalność była realizowana w innych modułach funkcjonalnych (np. anty-malware jako moduł obejmujący anty-spyware). Zamawiający dopuszcza rozwiązania, w których moduł/funkcjonalność Anty-Spyware jest częścią moduły/funkcjonalności Anty-Virus. Zamawiający wymaga, aby moduł/funkcjonalność Anty-Virus był uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł/funkcja Anty-Virus, który prowadzi również inspekcję Anty-Spyware uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

Pytanie nr 9 : ***Dotyczy Opisu przedmiotu zamówienia IV „Wymagania ochrony IPS,AV, anty-spyware, URL, zero-day" pkt. 12***

Takie wyodrębnienie funkcjonalności/modułu AntySpyware od AntyVirus występuje wyłącznie w rozwiązaniu producenta PaloAlto Networks. Pozostali producenci ochronę AntySpyware wykonują w module/funkcjonalności AntyVirus lub IPS, bez widocznego ich rozdzielenia. Wymaganie to więc w jednoznaczny sposób faworyzuje rozwiązanie PaloAlto Networks, i blokuje możliwość zaoferowania innych konkurencyjnych i wielu przypadkach lepszych rozwiązań, co jest niezgodne z ustawą i postępowaniach publicznych.

Rozumiemy, że intencją Zamawiającego jest skuteczna ochrona przed atakami typu Spyware, a nie jedynie zakup rozwiązania PaloAlto. Intencją Oferenta jest zaoferowanie wiodącego systemu bezpieczeństwa NGFW posiadającego wiele niezależnych certyfikacji i rekomendacji. Jest to rozwiązanie chroniące przez atakami typu Spyware, lecz posiadające funkcjonalność AntySpyware zintegrowaną z funkcjonalnością AntyVirus. Prosimy zatem o usunięcie wymagania lub jednoznaczne potwierdzenie iż Zamawiający dopuszcza rozwiązania w których moduł/funkcjonalność AntySpyware jest częścią modułu/funkcjonalności AntyVirus, a baza sygnatur AntyVirus zawiera sygnatury AntySpyware.lecz w razie potrzeby umożliwia również tworzenie ręczne sygnatur AntySpyware.

Odpowiedź : ***Zamawiający sprecyzował w SIWZ minimalne wymagania dla urządzenia stanowiącego przedmiot przetargu. Zamawiający określił te wymagania w sposób przejrzysty i nie wymagający dodatkowych wyjaśnień. Żądanie ich usunięcia nie spowoduje zwiększenia konkurencyjności, gdyż praktycznie wszyscy liczący się producenci posiadają urządzenia o funkcjonalności spełniającej wymagania Zamawiającego.***

Wymagania dotyczące silnika i sygnatur anty-spyware są wymaganiami funkcjonalnymi – i tutaj Zamawiający posłużył się ogólnie przyjętą taksonomią. Jednocześnie w innych wymaganiach SIWZ Zamawiający dopuścił aby ta funkcjonalność była realizowana w innych modułach funkcjonalnych (np. anty-malware jako moduł obejmujący anty-spyware). Zamawiający dopuszcza rozwiązania, w których moduł/funkcjonalność Anty-Spyware jest częścią moduły/funkcjonalności Anty-Virus. Zamawiający wymaga, aby moduł/funkcjonalność Anty-Virus umożliwiał ręczne tworzenie sygnatur anty-spyware. Nie jest dopuszczalne, aby moduł/funkcja Anty-Virus, który prowadzi również inspekcję Anty-Spyware stanowiła zamkniętą bazę opisów zagrożeń.

Pytanie nr 10 : ***dotyczy Opisu przedmiotu zamówienia IV „Wymagania ochrony IPS,AV, anty-spyware, URL, zero-day" pkt. 16***

Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Czy jako równoważne zostanie potraktowane rozwiązanie, gdzie na bazie współpracy z dedykowanym serwerem logowania tworzona jest lista skompromitowanych użytkowników oraz programowane są automatyczne akcje neutralizujące zagrożenie?

Odpowiedź : ***Tak. Zamawiający dopuszcza jako rozwiązanie równoważne rozwiązanie, gdzie na bazie współpracy z dedykowanymi serwerami fizycznymi tworzona jest lista skompromitowanych użytkowników oraz programowane są automatyczne akcje neutralizujące zagrożenie logowania. W przypadku stosowanie rozwiązań tego typu Zamawiający wymaga spełnienia dodatkowych wymagań wskazanych poniżej:***

Ze względu na to, iż Zamawiający nie posiada zwirtualizowanych zasobów obliczeniowych umożliwiających instalację i uruchomienie maszyn wirtualnych Oferent dostarczy rozwiązanie wykorzystujące fizyczne urządzenia, które będą wyprodukowane przez tego samego producenta co producent oferowanego Firewalla, będą objęte kontraktem serwisowym Producenta o tym samym okresie trwania, co kontrakty serwisowe oferowanych Firewalli oraz będę wyposażone w redundantne zasilacze.
Podobnie jak urządzenia firewall dodatkowy system musi być dostarczony jako redundantna para urządzeń fizycznych.

Pytanie nr 11 : ***dotyczy Opisu przedmiotu zamówienia IV „Wymagania ochrony IPS,AV, anty-spyware, URL, zero-day" pkt. 17***

Czy Zamawiający dopuści, jako równoważne rozwiązanie, które weryfikuje i blokuje dostęp do złośliwych serwisów webowych (phishing) tym samym chroniąc wewnętrzne poświadczenia użytkowników ?

Odpowiedź : ***Zamawiający zgadza się na dopuszczenie rozwiązania proponowanego przez Oferenta jako rozwiązanie równoważne.***

Pytanie nr 12 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dodatkowe: NAT,DoS, IPSEC, VPN, SSL VPN, QoS" pkt.5***

"System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach."

Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Prosimy o uproszczenie zapisu do konieczności wykrywania ataków w ruchu tunelowanym, tak jak jest to realizowane u większości topowych producentów NGFW.

Odpowiedź : ***Zamawiający zmienia zapisy SIZW. Nowe brzmienie wymagania: "System zabezpieczeń firewall musi umożliwiać wykrywanie oraz blokowania ataków w ruchu tunelowanym.***

Pytanie nr 13 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dodatkowe: NAT,DoS, IPSEC, VPN, SSL VPN, QoS" pkt. 7***

Czy obecnie Zamawiający używa mechanizmu uwierzytelniania typu SAML 2.0 ?
Prosimy o wylistowanie ilości tych systemów, typów systemów ilośc ilości użytkowników korzystających tego typu mechanizmu uwierzytelnienia w celu najlepszego dostosowania oferty.

Jeżeli na obecnym etapie Zamawiający nie korzysta z mechanizmu uwierzytelnienia SAML 2.0, proszę zatem o informacje, czy Zamawiający zaakceptuje rozwiązanie, które na etapie dostarczenia nie obsługuje mechanizmu uwierzytelnienia SAML 2.0 lecz posiada możliwość rozbudowy w razie potrzeby w przyszłości.

Odpowiedź : ***Zamawiający w najbliższym okresie planuje aktywne wykorzystywanie SAML 2.0 w celu zabezpieczenia dostępu do aplikacji UM z wykorzystaniem drugiego czynnika uwierzytelniającego. W związku z tym obsługa mechanizmy uwierzytelnienia SAML 2.0 musi być zaimplementowana w oferowanym przez Oferenta rozwiązaniu w momencie składania oferty. Zamawiający podtrzymuje zapisy SIWZ.***

Pytanie nr 14 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dodatkowe: NAT,DoS, IPSEC, VPN, SSL VPN, QoS" pkt. 7***

Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Prosimy o zawężenie listy mechanizmów do RADIUS, TACACS+, LDAP, Kerberos. Jeżeli wymagany jest SAML 2.0 prosimy o dopuszczenie wykorzystania dedykowanego serwera uwierzytelniania.

Odpowiedź : *Tak. Zamawiający dopuszcza jako rozwiązanie równoważne rozwiązanie z wykorzystaniem zewnętrznych fizycznych serwerów uwierzytelnienia. W przypadku stosowania rozwiązań tego typu Zamawiający wymaga spełnienia dodatkowych wymagań wskazanych poniżej:*

Ze względu na to, iż Zamawiający nie posiada zwirtualizowanych zasobów obliczeniowych umożliwiających instalację i uruchomienie maszyn wirtualnych Oferent dostarczy rozwiązanie wykorzystujące fizyczne urządzenia, które będą wyprodukowane przez tego samego producenta co producent oferowanego Firewalla, będą objęte kontraktem serwisowym Producenta o tym samym okresie trwania, co kontrakty serwisowe oferowanych Firewalli oraz będą wyposażone w redundatne zasilacze. Podobnie jak urządzenia firewall dodatkowy system wspierający identyfikację użytkowników musi być dostarczony jako redundantna para urządzeń fizycznych.

Pytanie nr 15 : *dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 3.*

Prosimy o dopuszczenie jako równoważnego rozwiązania, gdzie funkcjonalność ta może być zrealizowana z poziomu centralnej konsoli zarządzania dedykowanej przez producenta firewall'a instalowanej w środowisku wirtualizacyjnym Zamawiajacego.

Odpowiedź : *Tak. Zamawiający dopuszcza jako rozwiązanie równoważne rozwiązanie, gdzie funkcjonalność ta może być zrealizowana z poziomu centralnej konsoli zarządzania dedykowanej przez producenta firewall'a. W przypadku stosowania rozwiązań tego typu Zamawiający wymaga spełnienia dodatkowych wymagań wskazanych poniżej:*

Ze względu na to, iż Zamawiający nie posiada zwirtualizowanych zasobów obliczeniowych umożliwiających instalację i uruchomienie maszyn wirtualnych Oferent dostarczy rozwiązanie wykorzystujące fizyczne urządzenia, które będą wyprodukowane przez tego samego producenta co producent oferowanego Firewalla, będą objęte kontraktem serwisowym Producenta o tym samym okresie trwania, co kontrakty serwisowe oferowanych Firewalli oraz będą wyposażone w redundatne zasilacze. Podobnie jak urządzenia firewall dodatkowy system musi być dostarczony jako redundantna para urządzeń fizycznych.

Pytanie nr 16 : *dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 4.*

Prosimy o dopuszczenie jako równoważnego rozwiązania, gdzie funkcjonalność ta może być zrealizowana z poziomu centralnej konsoli zarządzania instalowanej w środowisku wirtualizacyjnym Zamawiajacego.

Odpowiedź : *Tak. Zamawiający dopuszcza jako rozwiązanie równoważne rozwiązanie, gdzie funkcjonalność ta może być zrealizowana z poziomu centralnej konsoli zarządzania dedykowanej przez producenta firewall'a. W przypadku stosowania rozwiązań tego typu Zamawiający wymaga spełnienia dodatkowych wymagań wskazanych poniżej:*

Ze względu na to, iż Zamawiający nie posiada zwirtualizowanych zasobów obliczeniowych umożliwiających instalację i uruchomienie maszyn wirtualnych Oferent dostarczy rozwiązanie wykorzystujące fizyczne urządzenia, które będą wyprodukowane przez tego samego producenta co producent oferowanego Firewalla, będą objęte kontraktem serwisowym Producenta o tym samym okresie trwania, co kontrakty serwisowe oferowanych Firewalli oraz będą wyposażone w redundatne zasilacze. Podobnie jak urządzenia firewall dodatkowy system musi być dostarczony jako redundantna para urządzeń fizycznych.

Pytanie nr 17 : *dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 5.*

Czy zamawiający dopuszcza zastosowanie JSON API?

Odpowiedź : ***Tak. Zamawiający dopuszcza jako równoważne zastosowania JSON API. Nowe brzmienie wymagania:***

"System zabezpieczeń firewall musi być wyposażony w interfejs XML API lub JSON API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

Pytanie nr 18 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 7.***

"System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos."

Czy Zamawiający zgadza się uprościć listę mechanizmów do LDAP, RADIUS, TACACS+?

Odpowiedź : ***Zamawiający zgadza się uprościć listę mechanizmów do LDAP, RADIUS i TACACS+.***

Pytanie nr 19 : ***dotyczy Opisu przedmiotu zamówienia IV. . „Wymagania dla zarządzania i raportowania" pkt. 8.***

"System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS)."

Czy jako równoważne zostanie potraktowane rozwiązanie, gdzie najpierw sprawdzane jest hasło na serwerze zdalnym, a jako backup stosowane jest hasło lokalne?

Odpowiedź : ***Zamawiający uzna za równoważne rozwiązanie, gdzie najpierw sprawdzane jest hasło na serwerze zdalnym, a jako backup stosowane jest hasło lokalne.***

Pytanie nr 20 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 9.***

Czy Zamawiający dopuści zastosowanie dedykowanej maszyny logującej i raportującej tego samego producenta ?

Odpowiedź : ***Tak. Zamawiający dopuszcza zastosowanie dedykowanych fizycznych maszyn logujących i raportujących tego samego producenta. W przypadku stosowania rozwiązań tego typu Zamawiający wymaga spełnienia dodatkowych wymagań wskazanych poniżej:***

Ze względu na to iż Zamawiający nie posiada zwirtualizowanych zasobów obliczeniowych umożliwiających instalację i uruchomienie maszyn wirtualnych Oferent dostarczy rozwiązanie wykorzystujące fizyczne urządzenia, które będą wyprodukowane przez tego samego producenta co producent oferowanego Firewalla, będą objęte kontraktem serwisowym Producenta o tym samym okresie trwania, co kontrakty serwisowe oferowanych Firewalli oraz będą wyposażone w redundantne zasilacze. Podobnie jak urządzenia firewall dodatkowy system musi być dostarczony jako redundantna para urządzeń fizycznych.

Pytanie nr 21 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 11.***

W dzisiejszych czasach zagrożenia cybernetyczne rozprzestrzeniają się z niebywałą prędkością, co pokazują chociaż by ostatnie głośne sprawy ataków typu Ramsomware. Jak wiadomo, ataki te wyrządziły najmniejsze szkody i straty finansowe tam, gdzie zasoby były zabezpieczone rozwiązaniami, producenci których w najkrótszym możliwym czasie dostarczali aktualizacji poprawek i sygnatur. W świetle tych wydarzeń, staje się jasne iż przeciąganie z wgrywaniem poprawek bezpieczeństwa niesie za sobą konkretne wymierne finansowo koszty, a co gorsza utratę reputacji instytucji. Dla tego też, w odróżnieniu od rozwiązań starszych generacji, nowoczesne systemy bezpieczeństwa posiadają na bieżąco(nawet kilak razy dziennie) aktualizowane bazy sygnatur i poprawek bezpieczeństwa by nadążyć za ciągle rozwijającymi się zagrożeniami. Pozostawienie możliwości przetestowania aktualizacji w odpowiedzialności administratora niesie ogromne ryzyko, gdyż administrator pojedynczej instytucji najczęściej nie posiada wystarczającej wiedzy na temat chronionych przez system NGFW systemów, a jeszcze mniej wiedzy o aktualnych zagrożeniach i istniejących aktualizacjach sygnatur dotyczących tych systemów. Dodatkowo, administrator nie będzie posiadał czasu by testować poprawki bezpieczeństwa i sygnatury aktualizowane kilka razy dziennie. Zważając na powyższe, w świecie dzisiejszych zagrożeń cybernetycznych to do wyspecjalizowanych laboratoriów producentów rozwiązań bezpieczeństwa należy dogłębna weryfikacja poprawności działania sygnatur i opublikowanie zweryfikowanej poprawki z możliwie najszybciej.

Prosimy zatem u usunięcie wymagania gdyż jest ono sprzeczne z ideą działania nowoczesnych systemów NGFW jak również jest sprzeczne z najlepszymi praktykami przyjętymi w branży.

Odpowiedź : ***Zamawiający przyjmuje wytłumaczenie Oferenta i wykreśla w/w wymaganie z SIWZ.***

Pytanie nr 22 : ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 11.***

"System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa."

Zapis wskazuje jednoznacznie na rozwiązanie firmy Palo Alto Networks. Prosimy o usunięcie zapisu jako niezgodnego z ustawą o postępowania publicznych lub dopuszczenie jako równoważnego rozwiązania, gdzie funkcjonalność ta może być realizowana z poziomu dedykowanego modułu logowania i raportowania.

Odpowiedź : ***Zamawiający uznaje jako równoważne rozwiązanie, gdzie funkcjonalność będąca przedmiotem tego pytania będzie realizowana z poziomu dedykowanego modułu logowania i raportowania.***

Pytanie nr 23: ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 16.***

Zapis wskazuje jednoznacznie na rozwiązanie firmy Palo Alto Networks. Inni producenci najczęściej tego rodzaju funkcjonalności relizują z poziomu dedykowanych narzędzi do logowania i raportowania. Przykładem takich rozwiązań jest LogCenter producenta Huawei, Firewall Log Analyzer producenta Dell, FortiAnalyzer producenta Fortinet, EventLog Analyzer producenta Cisco, SmartLog Software producenta Check Point.

Prosimy o usunięcie zapisu jako niezgodnego z ustawą o postępowania publicznych lub dopuszczenie jako równoważnego rozwiązania, gdzie funkcjonalność ta może być realizowana z poziomu dedykowanego modułu logowania i raportowania.

Odpowiedź : ***Zamawiający dopuszcza jako równoważne rozwiązanie, gdzie funkcjonalność ta może być realizowana z poziomu dedykowanego modułu logowania i raportowania.***

Pytanie nr 24: ***dotyczy Opisu przedmiotu zamówienia IV. „Wymagania dla zarządzania i raportowania" pkt. 17.***

Zapis wskazuje jednoznacznie na rozwiązanie firmy Palo Alto Networks. Inni producenci najczęściej tego rodzaju funkcjonalności realizują z poziomu dedykowanych narzędzi do logowania i raportowania. Przykładem takich rozwiązań jest LogCenter producenta Huawei, Firewall Log Analyzer producenta Dell, FortiAnalyzer producenta Fortinet, EventLog Analyzer producenta Cisco, SmartLog Software producenta Check Point.

Prosimy o usunięcie zapisu jako niezgodnego z ustawą o postępowania publicznych lub dopuszczenie jako równoważnego rozwiązania, gdzie funkcjonalność ta może być realizowana z poziomu dedykowanego modułu logowania i raportowania.

Odpowiedź : ***Zamawiający dopuszcza jako równoważne rozwiązanie, gdzie funkcjonalność ta może być realizowana z poziomu dedykowanego modułu logowania i raportowania.***

W związku z powyższym przesuwa się termin składania ofert **do dnia 13.03.2019r. do godz. 9:00.** Otwarcie ofert nastąpi w dniu ich składania, **tj. 13.03.2019r. godz. 9:30** w Urzędzie Miasta Gorzowa Wlkp. ,ul. Sikorskiego 5, pokój nr 2 (parter).

Treść odpowiedzi jest wiążąca dla wszystkich uczestników postępowania.

Z poważaniem

z up. PREZYDENTA MIASTA

Jacek Szymankiewicz

Zastępca Prezydenta Miasta