POLSKA AGENCJA PRASOWA S.A.

ul. Bracka 6/8, 00-502 Warszawa
tel. centr. (+48 22) 509 22 22
www.pap.pl

Warszawa, dn. 23 marca 2020 r.

DO WYKONAWCÓW

odpowiedzi na pytania złożone w postępowaniu o udzielenie zamówienia publicznego na dostawę do PAP S.A. urządzeń systemu bezpieczeństwa sieciowego typu firewall
(nr sprawy 06/20)

Zamawiający – Polska Agencja Prasowa S.A., zgodnie z art. 38 ust. 1 i 2 Ustawy z 29 stycznia 2004 r. – Prawo zamówień publicznych w odpowiedzi na pytania wykonawców złożone w przedmiotowym postępowaniu, odpowiada:

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.1.4 Zamawiający wymaga

> *System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000, 8 portów 1Gbps/10Gbps SFP/SFP+.*

Jednocześnie w punkcie I.1.5 Zamawiający pisze

> *System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż **5 Gbit/s** dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż **2,5 Gbit/s** dla kontroli zawartości*

Da się zauważyć, że Zamawiający oczekuje urządzenia dla którego wydajność całego urządzenia jest mniejsza niż wydajność pojedynczego portu wymaganego przez Zamawiającego.
Również widoczne jest iż, wymagania dotyczące ilości portów zostało skopiowane z karty katalogowej urządzenia PA-3250
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3200-series

Table 3: PA-3200 Series Hardware Specifications
I/O
PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)

Tak postawione wymaganie może nie odzwierciedlać rzeczywistej potrzeby Zamawiającego. Wymaganie to uniemożliwia zaoferowanie równoważnego rozwiązania innych producentów niż PA3250.
*Prosimy zatem o dopuszczenie rozwiązania alternatywnego, które posiada co najmniej **30 portów 1GE** które można agregować **w linki o łącznej przepustowości ponad 10G**,*
*lub prosimy o dopuszczenie rozwiązania alternatywnego, które posiada co najmniej **18 portów 1GE oraz 2 porty 10Gbps SFP/SFP+***

Odpowiedź

Wymóg posiadania portów SFP+ jest uzasadniony architekturą części rdzeniowej sieci i możliwościami fizycznego połączenia rozwiązania NGFW do obecnych przełączników rdzeniowych i dotyczy warstwy dostępu do sieci modelu TCP/IP. Zakłada się wdrożenie w pierwszej fazie dwóch portów SFP+ per firewall w celu zapewnienia redundancji. W przyszłości zakładane jest wdrożenie agregacji łącza co spowoduje wykorzystanie czterech portów SFP+ (pozostałe 4 porty przewidziane zostały jako redundancja lub wykorzystanie na przyszłe potrzeby zamawiającego).

Porty typu Ethernet wymagane są do połączeń operatorskich (3 lub porty + 3 lub 4 porty zapasowe), podłączenie sondy (1 port + 1 port zapasowy).

W ROZDZIAŁE XX pkt. I.1.4 specyfikacji przetargowej otrzymuje brzmienie:

„System zabezpieczeń firewall musi być wyposażony w co najmniej 10 portów Ethernet 10/100/1000, 8 portów 1Gbps/10Gbps SFP/SFP+. Zamawiający dopuszcza zastosowanie modułów rozszerzeń portów”

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.1.15 Zamawiający wymaga

Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.

Prosimy o wykreślenie tego zapisu z uwagi na jego nieprecyzyjność. Rozwiązania NGFW są oparte o dedykowane systemy operacyjne, pojęcie modułu nie jest tu sprecyzowane. Możemy operować pojęciem kernela lub procesów, ale to system operacyjny decyduje o efektywnym wykorzystaniu zasobów.

Odpowiedź

W ROZDZIAŁE XX pkt. I.1.15 specyfikacji przetargowej otrzymuje brzmienie:

„Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje profil IPS, sygnatury IPS ani dekodery protokołu IPS.”

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.1.20 Zamawiający wymaga:

System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Prosimy o równoważne dopuszczenie systemu, gdzie traktowanie aplikacji i filtra URL jako parametru polityki, dla których dowiązuje się profile ochronne AV, DNS, IPS.

Odpowiedź

W ROZDZIAŁE XX pkt. *I.1.20* specyfikacji przetargowej otrzymuje brzmienie:

„System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. Dopuszcza się system, który w ramach polityki bezpieczeństwa traktuje aplikacje i filtry URL jako parametr w regułach polityki bezpieczeństwa.”

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.*1.21 Zamawiający wymaga:*

> *System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.*

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 raczej 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 czy tif…

W związku z powyższym prosimy o usunięcie wymagania lub modyfikację wymagania na brzmiącą:

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 msoffice, pliki zaszyfrowane. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

Taka modyfikacja pozwoli na zaoferowanie rozwiązania więcej niż jednego producenta, i jednocześnie stworzy konkurencyjność składanych ofert.

Odpowiedź

W ROZDZIAŁE XX pkt. I.1.21 specyfikacji przetargowej otrzymuje brzmienie:

„System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, docx, ppt, pptx, xls, xlsx, rar, zip, exe, gzip, hta, pdf, tar, text/html, pliki zaszyfrowane. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

Wymaga się aby możliwa była jednoznaczna identyfikacja plików minimum narzędzi pakietu Office takich jak Word czy Excel.”

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.1.23 Zamawiający wymaga:

> *System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.*

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 **1.10** 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 **1.23** gdyż jest ono **sprzeczne z** wymaganiem **1.10** oraz funkcjonalność jest z zasady niezgodna i sprzeczna z ideą i najlepszymi praktykami wykorzystania systemów NGFW, które są tematem dzisiejszego postępowania.*

Odpowiedź

Zamawiający podtrzymuje zapis.

Interpretacja zapisu w następujący sposób*: „rozwiązanie pozwalające na kontynuowanie transmisji zainfekowanego pliku niesie potencjalne zagrożenie i jest niezgodne z ogólnie przyjętymi najlepszymi praktykami przyjętymi w branży"* jest mylna. Funkcja blokowania plików nie ma zastępować funkcjonalności IPS, antywirus czy innego profilu bezpieczeństwa. Zamawiający zakłada, że funkcja blokowania plików zadziała przed pobraniem pliku, a decyzja czy plik jest złośliwy czy nie zostanie podjęta w kolejnym kroku przez odpowiednie profile bezpieczeństwa i jeżeli plik jest złośliwy to takie pobranie zostanie zablokowane.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.2 Zamawiający wymaga:

> *System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.*

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 lub prosimy o dopuszczenie rozwiązania gdzie do tego celu będzie wykorzystany protokół RADIUS.

Odpowiedź

Stacji z systemami innymi niż MS Windows jest około 40.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.18 Zamawiający wymaga:

> *System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.*

Również w punkcie I.2.19 Zamawiający pisze:

> *System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).*

Oraz w punkcie I.2.20 Zamawiający pisze:

> *System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.*

Jedynie producent PaloAlto rozdziela moduł AntySpyware od modułu AntyVirus. Pozostało producenci NGFW plasujący się w kwadracie liderów Gartner moduł AntySpyware posiadają zintegrowany z modułem AntyVirus. Prosimy zatem o potwierdzenie iż Zamawiający dopuści rozwiązanie w którym moduł AntySpyware jest częścią modułu AntyVirus i/lub IPS, Moduł/funkcjonalność AntyVirus i/lub IPS zawierający sygnatury AntySpyware będzie uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł/funkcja AntyVirus i/lub IPS który prowadzi również inspekcję AntySpyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa) oraz umożliwia tworzenie sygnatur AntySpyware w module IPS.

Odpowiedź

Zamawiający istnienie funkcjonalności anty-spyware jako części profilu IPS lub antywirus. Wymagana jest możliwość tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.3 Zamawiający wymaga:

> *System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.*

Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Prosimy o uproszczenie zapisu, gdzie wystarczającym będzie rozpoznawanie adresów z nagłówków XFF, a uwierzytelniania użytkownika dopuszczalne będzie per sesja.

Odpowiedź

W ROZDZIAŁE XX pkt. I.2.3 specyfikacji przetargowej otrzymuje brzmienie:

> *„System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. W logach wymagana jest widoczność użytkownika inicjującego ruch do proxy”*

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.25 Zamawiający wymaga:

> *System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych*

w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

Pragniemy zwrócić uwagę, że wymaganie to jest sprzeczne z wymaganiem 1.10 gdzie Zamawiający 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 **2.25** gdyż jest ono **sprzeczne z** wymaganiem **1.10** oraz funkcjonalność jest z zasady niezgodna i sprzeczna z ideą i najlepszymi praktykami wykorzystania systemów NGFW, które są tematem dzisiejszego postępowania lub o dopuszczenie rozwiązania, gdzie na bazie współpracy z dedykowanym serwerem logowania tworzona jest lista skompromitowanych użytkowników oraz programowane są automatyczne akcje neutralizujące zagrożenie?*

Odpowiedź

W ROZDZIAŁE XX pkt. I.2.25 specyfikacji przetargowej otrzymuje brzmienie:

„System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów i/lub użytkowników biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. Dopuszcza się, aby taka funkcja realizowana była na systemie logowania i zarządzania firewallami"

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.26 Zamawiający wymaga:

System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.

Wymaganie w danej postaci może być spełnione tylko przez rozwiązanie producenta Palo Alto.

Prosimy dopuszczenie jako rozwiązanie równoważne, które weryfikuje i blokuje dostęp do złośliwych serwisów webowych (phishing) tym samym chroniąc poświadczenia użytkowników.

Odpowiedź

W ROZDZIAŁE XX pkt. I.2.26 specyfikacji przetargowej otrzymuje brzmienie:

„System zabezpieczeń firewall musi umożliwiać blokowanie stron WWW i serwisów identyfikowanych jako phishing"

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.26 Zamawiający wymaga:

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

Zwracamy uwagę, iż wymaganie w takiej postaci może być spełnione tylko przez rozwiązanie producenta Palo Alto.

Warto zaznaczyć, iż aby skorzystać z funkcjonalności opisanej w tym wymaganiu, Zamawiający musi zakupić dwa jednakowych rozwiązania Sandbox co wydaje się mało racjonalne.

Jeżeli intencją Zamawiającego jest rozbudowa o prywatny system „Sand-Box” w przyszłości, prosimy o modyfikację wymagania na brzmiące:

„ Musi istnieć możliwość integracji z prywatnym systemem typu "Sand-Box". W przypadku integracji z prywatnym systemem typu „Sand-Box” system NFGW w połączeniu z prywatnym systemem „Sand-Box” musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie skanowanych plików pomiędzy publicznym i prywatnym systemem typu "Sand-Box".

Odpowiedź

W ROZDZIAŁE XX OPZ punkt I.2.29 Zamawiający dopuszcza zmianę:

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

Zamawiający dokonał już zmiany zapisu na:

„Integracja z zewnętrznymi systemami typu "Sand-Box", po rozbudowaniu systemu poprzez zakupienie dodatkowych licencji, musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".

Jednak dopuszcza możliwość modyfikacji na:

„Musi istnieć możliwość integracji z prywatnym systemem typu "Sand-Box". W przypadku integracji z prywatnym systemem typu „Sand-Box” system NFGW w połączeniu z prywatnym systemem „Sand-Box” musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie skanowanych plików pomiędzy publicznym i prywatnym systemem typu "Sand-Box".”

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.2.30 Zamawiający wymaga:

> *Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.*

Zwracamy uwagę, iż wymaganie w takiej postaci może być spełnione tylko przez rozwiązanie producenta Palo Alto.

Działając zgodnie z wymaganiem 1.10 obecnego OPZ, gdzie Zamawiający wymaga by system działał zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone, prosimy o dopuszczenie rozwiązania, które pozwala na skonfigurowanie wysyłania do skanowania prze Sand-Box wszystkich wspieranych plikow i e.w. dodanie wyjątków, które pliki mają być wułączone ze skanowana przez Sand-box (np. exe, msoffice, java, jpeg, zip, rar, tar, bat, pdf, inne).

Odpowiedź

W ROZDZIAŁE XX pkt. I.2.30 specyfikacji przetargowej otrzymuje brzmienie:

„Administrator musi mieć możliwość konfiguracji rodzaju pliku (np. exe, dll, pdf, msofffice, java, jpg, swf, apk), oraz reguły w polityce bezpieczeństwa do określenia ruchu poddanego analizie typu „Sand-Box”.”

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.3.5 Zamawiający wymaga:

> *Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.*

Prosimy o informacje czy użytkownicy mobilni Zamawiającego korzystają z urządzeń z systemami operacyjnymi Windows, Android, iOC, Mac OS.

Jaką ilość jednocześnie połączonych użytkowników powinien obsługiwać system?

Odpowiedź

Użytkownicy korzystają z urządzeń z systemami operacyjnymi Windows, Android, iOS, Mac OS. Liczba użytkowników potrzebujących dostępu zdalnego jednocześnie wynosi do 1100.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.3.6 Zamawiający wymaga:

> *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.*

Wymaganie w takiej postaci może być spełnione tylko przez rozwiązanie producenta Palo Alto. Prosimy o uproszczenie zapisu do konieczności wykrywania ataków w ruchu tunelowanym.

Odpowiedź

Zamawiający wykreśla punkt I.3.6.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.3.8 Zamawiający wymaga:

> *System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.*

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 dopuszcza rozwiązania nie wspierające SAML 2.0, obecnie jednak wymagana jest informacja typu road-map od producenta kiedy i w jaki sposób taka funkcjonalność będzie wspierana.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.3 Zamawiający wymaga:

> *System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.*

Prosimy o dopuszczenie systemu, dla którego wymaganie to będzie realizowane z poziomu systemu Zarządzania, który również jest częścią dzisiejszego postępowania.

Odpowiedź

Zamawiający dopuszcza zmianę, w której system zarządzania realizuje dostęp na podstawie RBAC (role based access control) i umożliwia edytowanie konfiguracji kandydackiej przez wielu

administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami Wymaga się, aby w przypadku awarii systemu zarządzania prace dokonywane przez wielu administratorów miały ten sam charakter co przed awarią zatem system zarządzania dla takiego rozwiązania musi być w postaci redundantnej.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.4 Zamawiający wymaga:

> *System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji*

Prosimy o dopuszczenie systemu, dla którego wymaganie to będzie realizowane z poziomu systemu Zarządzania, który również jest częścią dzisiejszego postępowania.

Odpowiedź

Zamawiający dopuszcza się zmianę, w której system zarządzania realizuje dostęp na podstawie RBAC (role based access control) i pozwala na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. Wymaga się, aby w przypadku awarii systemu zarządzania prace dokonywane przez wielu administratorów miały ten sam charakter co przed awarią zatem system zarządzania dla takiego rozwiązania musi być w postaci redundantnej.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.5 Zamawiający wymaga:

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

Prosimy o dopuszczenie systemu, który wyposażony w interfejs REST API.

Odpowiedź

W ROZDZIAŁE XX pkt. I.5.5 specyfikacji przetargowej otrzymuje brzmienie:

> *„System zabezpieczeń firewall musi być wyposażony w interfejs XML API lub REST 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

W ROZDZIAŁE XX OPZ w punkcie I.5.7 Zamawiający wymaga:

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

Prosimy o dopuszczenie, jako alternatywnego, rozwiązania, które umożliwia uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i SAML.

Odpowiedź

W ROZDZIAŁE XX pkt. *I.5.7* specyfikacji przetargowej otrzymuje brzmienie:

> *„System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+”*

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.9 Zamawiający wymaga:

> *System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania,*

analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.

Prosimy o dopuszczenie rozwiązania które nie posiada dysku przeznaczonego do przechowywania logów, lecz logi będą przechowywane na centralnym systemie logowania, który również jest częścią postępowania.

Odpowiedź

Wymaga się, aby w razie awarii centralnego systemu zarządzania logi były zapisywane lokalnie na firewallu. Jeżeli oferowany firewall nie spełnia wymogu należy zaoferować system zarządzania w postaci redundantnej wraz z redundancją przechowywania logów.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.11 Zamawiający wymaga:

System zabezpieczeń firewall musi zapewniać mechanizm pozwalający na sprawdzenie podczas procesu instalacji nowej bazy sygnatur aplikacyjnych, które reguły bieżącej polityki bezpieczeństwa, polityki PBR (policy based routing) oraz polityki QoS wykorzystują sygnatury aplikacyjne modyfikowane w ramach bieżącej aktualizacji baz sygnatur.

Wymaganie w takiej postaci może być spełnione tylko przez rozwiązanie producenta Palo Alto i uniemożliwia zaoferowanie Zamawiającemu rozwiązań innych topowych producentów.

W związku z powyższym prosimy o usunięcie wymagania.

Odpowiedź

Zamawiający wykreśla punkt I.5.11

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.12 Zamawiający wymaga:

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

Prosimy o dopuszczenie rozwiązania, dla którego funkcjonalność ta będzie realizowana z poziomu systemu centralnego logowania, który również jest częścią postępowania.

Odpowiedź

Dopuszcza się możliwość wysyłania logów per polityka do różnych serwerów Syslog z centralnego systemu zarządzania. Wymaga się, aby w razie awarii centralnego systemu zarządzania wysyłanie logów było kontynuowane więc, należy zaoferować system zarządzania w postaci redundantnej wraz z redundancją przechowywania logów.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.13 Zamawiający wymaga:

System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

Prosimy o dopuszczenie rozwiązania, dla którego funkcjonalność ta będzie realizowana z poziomu systemu centralnego logowania, który również jest częścią postępowania.

Odpowiedź

Dopuszcza się możliwość selektywnego wysyłania logów bazując na atrybutach z centralnego systemu zarządzania. Wymaga się, aby w razie awarii centralnego systemu zarządzania wysyłanie logów było kontynuowane więc, należy zaoferować system zarządzania w postaci redundantnej wraz z redundancją przechowywania logów.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie I.5.16 Zamawiający wymaga:

> *System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.*

Prosimy o dopuszczenie rozwiązania, dla którego funkcjonalność ta będzie realizowana z poziomu systemu centralnego logowania, który również jest częścią postępowania.

Odpowiedź

Dopuszcza się taką funkcjonalność z centralnego systemu zarządzania. Wymaga się, aby w razie awarii centralnego systemu zarządzania wysyłanie logów było kontynuowane więc, należy zaoferować system zarządzania w postaci redundantnej wraz z redundancją przechowywania logów.

Pytanie

W ROZDZIAŁE XX OPZ w punkcie II.3 Zamawiający wymaga:

> *System zarządzania, logowania i raportowania musi umożliwiać dodanie dodatkowej przestrzeni dyskowej przeznaczonej na logowanie.*

Czy Zamawiający dopuści rozwiązanie, które nie posiada możliwości zwiększenia przestrzeni dyskowej w przyszłości, ale już za etapie dostawy będzie zapewniło 8 TB dodatkowej przestrzeni na logi.

Odpowiedź

Zamawiający dopuszcza takie rozwiązanie. Jeżeli rozwiązanie nie dopuszcza dołożenia przestrzeni dyskowej to winna istnieć możliwość zakupu i wdrożenia sprzętu lub maszyn wirtualnych realizujących funkcję zbierania logów, które to pozwolą na zbieranie więcej niż 8 TB logów w przyszłości i ich wyskalowanie.

Pytanie

Prosimy o dokładną informację co Wykonawca ma zawrzeć w Szczegółowym opisie oferowanego przedmiotu zamówienia (ofercie merytorycznej). Czy mają to być broszury produktowe producenta opisujące oferowane produkty?

Odpowiedź

W opisie oferowanego przedmiotu zamówienia powinny znaleźć się dokumenty potwierdzające spełnienie wymagań postawionych w Opisie Przedmiotu Zamówienia takie jak: szczegółowe broszury produktowe i wydajności (w szczególności informacje na temat przepustowości, ilości sesji, ilości reguł polityki bezpieczeństwa, ilości reguł NAT, ilości obiektów, ilości własnych wpisów i kategorii URL, ilości tuneli VPN S-to-S i C-to-S, itd.), opis szczegółowy, opis oferowanych usług i zakres świadczonej ochrony.

Podsumowując: szczegółowy opis musi pozwolić Zamawiającemu na ocenę oferty czy jej treść jest zgodna z treścią specyfikacji przetargowej.

Pytanie

Dotyczy SIWZ Rozdział IX kryterium 2. - S

> *W chwili obecnej jedynie Palo Alto Networks otrzymuje komplet punktów w powyższym kryterium. Raporty NSS Labs nie są do końca miarodajne ponieważ zależą często od wstępnej konfiguracji urządzeń a nie ich możliwości. Tak na przykład w 2018 roku producent Check Point w powyższym raporcie miał zaledwie 25% aby w 2019 roku mieć już 97,4%.*

Również Palo Alto w 2018 roku zajęło dopiero czwartą lokatę w tym raporcie. Producenci firewall nie zmieniają w ciągu 1 roku swoich systemów aby nastawały takie różnice w ich ocenie. Uzależniając kryterium akurat od tego raportu i akurat w 2019 roku wskazuje literalnie na urządzenia Palo Alto. Jeżeli Zamawiający chce przyznać punkty za wysoki poziom bezpieczeństwa systemu firewall prosimy o zmianę wymagania na wymaganie najczęściej pojawiające się w kryteriach przetargów publicznych na systemy firewall tzn. od obecności w kwadracie Gartner – Magic Quadrant for Network Firewalls. Poniżej przesyłamy propozycję zmiany wymagania 2. – S. Bardzo prosimy o jego zmianę celem umożliwienia konkurencyjności złożenia oferty na topowe rozwiązania dostępne na rynku:

Skuteczność wykrywania zagrożeń przez system, zgodnie z Raportem Gartnera Magic Quadrant for Enterprise Network Firewalls:

- *w okresie trzech ostatnich lat przed wszczęciem niniejszego postępowania obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie Leaders przez co najmniej 3 (trzy) lata z rzędu - 10 pkt*
- *w okresie trzech ostatnich lat przed wszczęciem niniejszego postępowania obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie Leaders lub Challengers przez co najmniej 3 (trzy) lata z rzędu - 5 pkt*
- *Brak obecności w raportach Gartner Magic Quadrant for Enterprise Network Firewalls lub obecność niespełniająca powyższych dwóch punktów – 0 pkt*

Odpowiedź

Zamawiający pozostaje przy kryterium raportu NSS Labs. Raport Gartner – Magic Quadrant for Network Firewalls jest raportem skupiającym się w bardzo dużym stopniu na umiejętności realizacji biznesu i wizji producentów. Jego tematem nie jest szczegółowość konfiguracji rozwiązania i analiza pod kątem dostępnych zasobów producenckich w temacie najlepszych praktyk w implementacji firewalli w środowisku korporacyjnym.