UNIA EUROPEJSKA
FUNDUSZ AZYLU, MIGRACJI I INTEGRACJI
Bezpieczna Przystań

Wojewoda Kujawsko-Pomorski

Kujawsko-Pomorski Urząd Wojewódzki w Bydgoszczy
Biuro Finansowo-Inwestycyjne
ul. Jagiellońska 3
85-950 Bydgoszcz

BFI.II.272.2.10.2020

Bydgoszcz, 12.10.2020 r.

WYKONAWCY
biorący udział w postępowaniu
na Dostawę urządzeń brzegowych firewall dla Kujawsko-Pomorskiego Urzędu Wojewódzkiego w Bydgoszczy (Zadanie realizowane jest w ramach projektu pt. "Wzmocnienie zdolności administracyjnych Wojewody Kujawsko-Pomorskiego w procesie integracji obywateli państw trzecich - etap II", nr projektu 1/10-2019/OG-FAMI, współfinansowanego z Programu Krajowego FUNDUSZU AZYLU, MIGRACJI I INTEGRACJI)

ODPOWIEDŹ
na zapytania w sprawie SIWZ

Szanowni Państwo,

Uprzejmie informujemy, iż w dniach 08-12.10.2020 r. do Zamawiającego wpłynęły prośby o wyjaśnienie zapisów specyfikacji istotnych warunków zamówienia, w postępowaniu prowadzonym na podstawie przepisów ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych (Dz. U. z 2019 r. poz. 1843 z późn. zm.) w trybie **przetargu nieograniczonego**, na:
Dostawę urządzeń brzegowych firewall dla Kujawsko-Pomorskiego Urzędu Wojewódzkiego w Bydgoszczy (Zadanie realizowane jest w ramach projektu pt. "Wzmocnienie zdolności administracyjnych Wojewody Kujawsko-Pomorskiego w procesie integracji obywateli państw trzecich - etap II", nr projektu 1/10-2019/OG-FAMI, współfinansowanego z Programu Krajowego FUNDUSZU AZYLU, MIGRACJI I INTEGRACJI).

Treść zapytań i stanowisko (wyjaśnienia) Zamawiającego w przedmiotowych kwestiach są następujące:

1. Pytanie do punktu 3.24i
   i) AntyMalware (Emulacja zagrożeń Sandbox)
   a. System musi zapewniać ochronę przed nieznanym złośliwym oprogramowaniem, na zasadzie analizy behawioralnej. Cała ochrona realizowana jest poprzez analizę nieznanych obiektów w specjalnie wyizolowanym, wirtualnym środowisku. Zamawiający dopuszcza wykonywanie emulacji plików w chmurze producenta z zachowaniem regulacji wynikających z GDPR
   b. System musi zapewniać ochronę w czasie rzeczywistym
   c. System musi mieć możliwość blokowania poczty zawierającej podejrzane załączniki do czasu zakończenia ich analizy
   Czy Zamawiający dopuszcza rozwiązanie, które stawia na priorytet dostarczenie poczty, która nie musi mieć możliwości blokowania poczty zawierającej podejrzane załączniki, które będą pierwszy raz analizowane do czasu zakończenia ich analizy? Taka analiza może być czasochłonna, więc kolejne takie załączniki będą blokowane. Oczywistym jest, że administrator będzie powiadomiony o pozytywnym rezultacie analizy poczty, która zawiera złośliwy kod typu zero-day.

Odp.: Zamawiający nie dopuszcza takiego rozwiązania.

2. Pytanie do punktu 3.26
   Zarządzanie firewall musi zapewniać:

Administracja musi być możliwa poprzez linię poleceń (CLI) oraz interfejs graficzny (GUI) w czasie rzeczywistym.
Poprzez administrację należy rozumieć konfigurację polityk bezpieczeństwa (polityka zapory sieciowej, VPN, polityka ochrony antywirusowej, ochrony przed atakami sieciowymi, kontrola aplikacji), zarządzanie kontami administratorów i użytkowników, obsługę zdarzeń generowanych przez moduły zapór sieciowych
Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP (Active Directory), RADIUS, TACACS+ i Kerberos
Urządzenie musi wspierać zarządzanie poprzez bezpieczne kanały komunikacji - HTTPS, SSH, konsolę
Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub email
Rozwiązanie powinno umożliwiać edytowanie polityk w trybie online
Tworzenie kont administracyjnych o różnych uprawnieniach
Rozwiązanie powinno posiadać możliwość monitorowania logów w czasie rzeczywistym
Zamawiający w tym punkcie wymienił szereg różnych funkcjonalności, które musi zapewnić firewall. Czy Zamawiajcy się zgodzi na rozwiązanie, które zapewnia większość z nich, jednakże nie wspiera TACACS+? TACACS+ został opracowany i jest własnością CISCO System.

Odp.: Zamawiający dopuszcza rozwiązania, które nie wspiera TACACS +.

3. Pytanie do punktu 3.26
Logowanie i raportowanie:
System musi umożliwiać składowanie i archiwizację logów, gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, wykorzystywanych aplikacjach sieciowych, wykrytych atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych, itd.
Powiązać powyższe zdarzenia z nazwami użytkowników
Zapewnić generowanie raportów
Zapewnić export zgromadzonych logów do zewnętrznych systemów składowania danych
Generować raporty do plików pdf
Generować statystyki wykorzystania łącza internetowego, np. w ujęciu dziennym, tygodniowym, miesięcznym czy rocznym
Zamawiający w tym punkcie wymienił szereg różnych funkcjonalności, które musi zapewnić firewall. Czy Zamawiający się zgodzi na rozwiązanie, które zapewnia większość z nich, jednakże nie wspiera protokołu IM oraz generowania raportów do plików pdf?

Odp.: Zamawiający nie dopuszcza rozwiązań, które nie wspierają protokołu IM oraz generowania raportów do pliku pdf.

4. Dot. punktu 3.9.e:
e) Zamawiający wymaga aby dostarczone urządzenia zapewniały obsługę minimum 2 wirtualnych routerów
Połączenia VPN (Site-to-Site, Klient): 50
Liczba VLANów per urządzenie / per interfejs (standard IEEE802.1q): 1000
Liczba obsługiwanych użytkowników: nieograniczona
Czy Zamawiający zgodzi się na urządzenie, które nie wspiera wirtualnych routerów, ale realizuje wszystkie funkcjonalności, jak:
Połączenia VPN (Site-to-Site, Klient): 50
Liczba VLANów per urządzenie / per interfejs (standard IEEE802.1q): 1000
Liczba obsługiwanych użytkowników: nieograniczona

Odp.: Zamawiający nie dopuszcza urządzeń, które nie wspierają wirtualnych firewalli lub routerów.

5. Dot. punktu 3.10:
Sieć:
Zarządzanie adresami IP: Static, DHCPv4/v6 Serwer, Klient, Relay, DDNS, DNS Forwarding
IP Routing: BGPv4/v6, OSPFv2/v3, RIPv2, Static Routes, IP Policy Based Routing (PBR)
Translacja adresów: NAT, PAT
Enkapsulacja: Ethernet, 802.1Q VLANs, GRE; PPPoE, IP in IP Bridging, Bonding (802.3ad)
VPN: IPsec (IKEv1/v2, AES256, SHA256, 3DES), PPTP, L2TP, IPsec NAT Traversal

Dostępność HA: Firewall / NAT Failover, VRRP, IPsec VPN Clustering
Zarządzanie / Autoryzacja: CLI, WebGUI, SSHv2, Radius, Active Directory, TACACS+, Kerberos
Zamawiający w tym punkcie wymienił szereg różnych funkcjonalności. Czy Zamawiający się zgodzi na rozwiązanie, które zapewnia większość z nich, jednakże nie wspiera: IP in IP Bridging, VRRP, TACACS+ ze względu na to, że te mechanizmy prawdopodobnie nigdy nie będą użyte?

Odp.: Zamawiający zgodzi się na rozwiązanie, gdzie urządzenie nie wspiera IP in IP Bridging, VRRP oraz TACACS+.

6. Dot. punktu 3.24b
b) Antywirus:
a. Aktualizacja sygnatur powinna odbywać się automatycznie
b. Powinien posiadać możliwość przeprowadzania kwarantanny e-mail
c. Rozwiązanie musi posiadać możliwość tworzenia wyjątków (biała lista)
d. Rozwiązanie powinno wykrywać i blokować spyware
e. Rozwiązanie powinno skanować pliki skompresowane (zip, tar, rar, gzip) z wieloma poziomami kompresji
f. Rozwiązanie musi posiadać wsparcie dla głównych protokołów http, https, ftp, smtp, pop3, imap
Zamawiający w tym punkcie wymienił szereg różnych funkcjonalności Antywirusa.
Czy Zamawiający się zgodzi na rozwiązanie, które zapewnia większość z nich, jednakże nie wspiera kwarantanny i skanowania dla imap?

Odp.: Zamawiający dopuszcza brak kwarantanny lecz nie dopuszcza braku skanowania dla imap.

7. Dot. punktu 3.24c
c) AntySpam:
a. Aktualizacja sygnatur powinna odbywać się automatycznie
b. AntySpam powinien zapewniać możliwość kwarantanny e-mail
c. Rozwiązanie powinno umożliwiać blokowanie spamu z różnych domen
Zamawiający w tym punkcie wymienił szereg różnych funkcjonalności AntySpam.
Czy Zamawiający się zgodzi na rozwiązanie, które zapewnia większość z nich, jednakże nie wspiera kwarantanny?

Odp.: Zamawiający dopuszcza rozwiązanie, które nie wspiera kwarantanny.

8. W punkcie 3.3 Zamawiający wymaga aby urządzenia pełniące rolę zapory sieciowej były wyposażone w dysk SSD o pojemności nie mniejszej niż 240GB. W przypadku urządzeń pełniących rolę zapory sieciowej, wielkość dysku nie wpływa na wydajność i poziom bezpieczeństwa zapewnianego przez urządzenie. Pozostawienie takiego wymogu niewiele zmienia w sensie ochrony sieci a znacznie a w znaczący sposób ogranicza możliwość zaoferowania korzystniejszych pod względem funkcjonalnym i ekonomicznym rozwiązań. Mając na uwadze powyższe prosimy o informację
Czy Zamawiający zgodzi zmianę wymagania w zakresie wielkości zastosowanego dysku SSD z 240GB na 64GB?

Odp.: Zamawiający dopuszcza urządzenia wyposażone w dysk o wielkości min. 64GB.

9. W punkcie 3.9.e Zamawiający wymaga aby dostarczone urządzenia zapewniały obsługę minimum 2 wirtualnych routerów.
Czy Zamawiający uzna za spełnienie tego wymagania jeśli zamiast tego z każdym z urządzeń otrzyma dodatkowo możliwość uruchomienia dodatkowego wirtualnego firewalla? Rozwiązanie takie zapewni mu znacznie większe możliwości, gdyż oprócz wirtualnego routera otrzyma w pełni funkcjonalny firewall z antywirusem, antyspaywarem, IPSem, firewallem aplikacyjnym i filtracją treści.

Odp.: Zmawiający dopuszcza takie rozwiązanie.

10. W punkcie 3.9.f i g Zamawiający wymaga aby dostarczone urządzenia miały wydajność nie mniej niż 5 Gbit/s dla kontroli firewall z włączoną funkcją IPS i nie mniej niż 2.5 Gbit/s dla kontroli zawartości.
Czy Zamawiający dopuszcza aby urządzenia miały wydajność nie mniej niż 3,4 Gbit/s dla kontroli firewall z włączoną funkcją IPS i nie mniej niż 2.8 Gbit/s dla kontroli zawartości?

Odp.: Zamawiający dopuszcza by urządzenie posiadało wydajność nie mniej niż 3,4 Gbit/s dla kontroli firewall z włączoną funkcją IPS.

11. W punkcie 3.9.h i i Zamawiający wymaga aby dostarczone urządzenia zapewniały obsługę minimum 2 000 000 połączeń przy 80 000 połączeń na sekundę.
Czy Zamawiający dopuszcza urządzenia, które zapewniają obsługę minimum 4 000 000 połączeń przy 40 000 połączeń na sekundę?

Odp.: Zamawiający dopuszcza urządzenia zapewniające obsługę min. 2 000 000 połączeń przy min. 40 000 połączeń na sekundę.

12. W punkcie 3.7 Zamawiający wymaga aby dostarczone urządzenia posiadały między innymi 4 porty 10Gigabit SFP+. Daje to sumaryczną wydajność połączenia 40Gbps, gdy tymczasem wymagana wydajność urządzenia to tylko 5 Gbps.
Czy Zamawiający dopuści urządzenie posiadające 2 porty 10Gigabit SFP+ ? Dwa porty zapewnią możliwość redundantnego połączenia i jednocześnie czterokrotny zapas w stosunku do wydajności.

Odp.: Zamawiający dopuszcza urządzenie posiadające 2 porty 10Gigabit SFP+.

13. W punkcie 3.9 Zamawiający wymaga aby liczba VLANów na urządzenia/interfejs wynosiła 1000. W przypadku firewalli użycie takiej ilości VLANów zdarza się ogromnie rzadko.
Czy Zamawiający dopuszcza urządzenie które wspiera do 500 interfejsów VLAN?

Odp.: Zamawiający dopuszcza urządzenia, które wspierją min. 500 interfejsów VLAN.

14. W punkcie 3.10 Zamawiający wymaga aby dostarczone urządzenia wspierały między innymi IP Routing: BGPv4/v6, OSPFv2/v3. BGPv6, OSPFv3 to protokoły routingu IPv6, który w jest jeszcze bardzo rzadko stosowany.
Czy Zamawiający dopuszcza urządzenia wspierające BGPv4, OSPFv2?

Odp.: Zamawiający dopuszcza urządzenie wspierające BGPv4, OSPFv2 (tj. bez wsparcia dla BGPv6, OSPFv3).

15. Czy Zamawiający dopuszcza rozwiązanie niewspierające protokołu VRRP (wymóg 3.10 OPZ). Realizowana protokołem redundancja zostanie zapewniona za pomocą klastra High Availability.

Odp.: Zamawiający dopuszcza rozwiązanie niewspierające protokół VRRP.

Z up. Dyrektora Generalnego
Kujawsko-Pomorskiego Urzędu Wojewódzkiego
w Bydgoszczy
Dyrektor
Biura Finansowo-Inwestycyjnego
Piotr Moskal