GMINA MICHAŁOWICE

Reguły, ul. Aleja Powstańców Warszawy 1
05-816 Michałowice

tel. **22 350 91 91** faks **22 350 91 01**
www.michalowice.pl e-mail: **sekretariat@michalowice.pl**
ePUAP: **/4ld31qr0t1/SkrytkaESP**

Reguły, 13 maja 2022 roku

IT.271.3.2022

Wykonawcy
biorący udział w postępowaniu

Dot. postępowania o udzielenia zamówienia publicznego nr IT.271.3.2022 pn.:
„Dostawa sieciowego urządzenia brzegowego UTM”

Zamawiający – Gmina Michałowice informuje, że zgodnie z zapisami w Rozdziale VI WYJAŚNIENIA DOTYCZĄCE TREŚCI ZAPYTANIA OFERTOWEGO udziela odpowiedzi na pytania, które zostały złożone do ww. postępowania.

Wniosek Oferenta do przedmiotowego postępowania:

Opis który został opracowany, którego wszystkie punkty łącznie wskazują bezpośrednio na model Fortinet Fortigate 201F co nie odpowiada zasadom uczciwej konkurencji, wnioskujemy o dopuszczenie parametrów równoważności.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

Propozycja 1:

Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.

Odpowiedź:

Zamawiający informuje, że tożsamy zapis jest już w OPZ:

„System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT oraz transparentnym.”

Propozycja 2:

System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000. System realizujący funkcję Firewall musi umożliwiać rozszerzenie dostępnych interfejsów o minimum 4 interfejsy optyczne 10GbE (SFP+)

Odpowiedź:

Zamawiający ponownie przeanalizował możliwe sposoby podłączenia systemu i w OPZ zawarł minimalne ilości i prędkości portów jakie powinien, aby w przyszłości zapewnić elastyczność rekonfiguracji w miarę modernizacji infrastruktury.

Zamawiający zmienia zapis w OPZ co do minimalnej ilości i rodzaju portów, Oferent może zaoferować urządzenie o większej ilości potów lub o portach szybszych jako równoważne.

przed zmianą:

„System realizujący funkcję Firewall musi dysponować minimum:
• 2 portami Gigabit Ethernet RJ-45 przeznaczonymi dla ruchu WAN,
• 12 portami Gigabit Ethernet RJ-45,
• 4 gniazdami SFP 1 Gbps,
• 2 gniazdami SFP+ 10 Gbps”

po zmianie:

„System realizujący funkcję Firewall musi dysponować minimum:
• 2 portami Gigabit Ethernet RJ-45 przeznaczonymi dla ruchu WAN,
• 8 portami Gigabit Ethernet RJ-45,
• 2 gniazdami SFP+ 10 Gbps”

Propozycja 3:

Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.

Odpowiedź:

Zamawiający planuje segmentację sieci i ocenia, że system zapewniający utworzenie minimum 200 wirtualnych interfejsów da wystarczającą elastyczność na przestrzeni kolejnych kilku lat użytkowania systemu. Na rynku dostępne są różne systemy i urządzenia renomowanych producentów posiadające taką funkcjonalność. Zamawiający podtrzymuje zapisy OPZ.

Propozycja 4:

W zakresie Firewall’a obsługa nie mniej niż 1 500 000 jednoczesnych połączeń oraz 79 000 nowych połączeń na sekundę.

Odpowiedź:

Oferent proponuje obniżenie wymaganej wydajności urządzenia o połowę dla parametru „jednoczesnych połączeń” i ponad 3 krotnie dla parametru „nowych połączeń na sekundę”.

Zamawiający nie zgadza się na takie obniżenie parametrów wydajnościowych systemu i podtrzymuje zapis OPZ.

Propozycja 5:

System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 120 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.

Odpowiedź:

Zamawiający chce uzyskać maksymalnie długi okres przechowywania logów i ocenia, że dysk o wskazanej w OPZ pojemności 450GB zapewni taka funkcjonalność. Zamawiający nie zgadza się na prawie czterokrotne zmniejszenie tego parametru i podtrzymuje zapisy OPZ. Zamawiający jednocześnie zaznacza, że już na początku wskazał możliwość dostawy systemu w postaci osobnych, platform sprzętowych lub aplikacji instalowanych na platformach ogólnego przeznaczenia co w ocenie zamawiającego jest tożsame z propozycją Oferenta.

Propozycja 6:

System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.

W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:

- Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego

- Generowanie co najmniej 25 różnych typów raportów

- System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania.

Odpowiedź:

Przedmiotem zamówienia nie jest zakup systemu raportowania, agregacji i przeglądania logów. Zamawiający nie wprowadza tego zapisu do OPZ co jednocześnie nie wyklucza rozwiązań które taką funkcjonalność posiadają.

Propozycja 7:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection

Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS).

System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.

Poufność danych - IPSec VPN oraz SSL VPN

Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

Kontrola stron Internetowych – Web Filter [WF]

Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)

Kontrola pasma oraz ruchu [QoS i Traffic shaping]

Kontrola aplikacji oraz rozpoznawanie ruchu P2P o Analiza ruchu szyfrowanego protokołem SSL

Odpowiedź:

OPZ opublikowany przez Zamawiającego zawiera wszystkie zaproponowane zapisy.

Propozycja 8:

1. Wydajność systemu Firewall minimum 30 Gbps
2. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2,9 Gbps
3. Wydajność ochrony przed atakami (IPS) minimum 15 Gbps
4. Wydajność VPN IPSec, nie mniej niż 4,5 Gbps

Odpowiedź:

Zamawiający w OPZ zaproponował analogiczne zapisy wydajnościowe

1. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B
2. Wydajność skanowania ruchu mieszanego (Enterprise Traffic Mix) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
3. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu mieszanego (Enterprise Traffic Mix) - minimum 5 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 13 Gbps.

przy czym dla pozycji pierwszej i trzeciej określił niższe wymagania od proponowanych i zapis podtrzymuje, w przypadku pozycji czwartej nie zgadza się na prawie trzy krotne obniżenie parametru wydajnościowego. W przypadku pozycji drugiej zmniejsza wymaganie do 2,9 Gbps przy założeniu że wydajność dotyczy włączonych wszystkich funkcji ochrony urządzenia (IPS, Application Control, Antywirus).

przed zmianą:

Wydajność skanowania ruchu mieszanego (Enterprise Traffic Mix) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.

po zmianie:

Wydajność skanowania ruchu mieszanego (Enterprise Traffic Mix) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2,9 Gbps.

Propozycja 9:

W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site;

Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem;

Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;

Praca w topologii Hub and Spoke oraz Mesh;

Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth;

Obsługa ssl vpn w trybach portal oraz tunel;

Odpowiedź:

OPZ opublikowany przez Zamawiającego zawiera wszystkie powyższe zaproponowane zapisy w dziale „Połączenia VPN" opublikowanej specyfikacji. Zawiera również dodatkowe parametry dotyczące technologii nowoczesnych połączeń VPN, jeżeli Oferent znajduje zapisy dyskryminujące jego ofertę prosimy o wskazanie ich wraz z uzasadnieniem.

Propozycja 10:

Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.

Odpowiedź:

Zamawiający zgadza się na zaproponowany zapis i usuwa z wymogu protokół PIM.

przed zmianą:

„W zakresie routingu rozwiązanie powinno zapewniać obsługę:
• Routingu statycznego,
• Policy Based Routingu,
• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM."

po zmianie:

„W zakresie routingu rozwiązanie powinno zapewniać obsługę:
• Routingu statycznego,
• Policy Based Routingu,
• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP."

Propozycja 11:

Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.

Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).

Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.

Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

Baza filtra WWW pogrupowana w min 50 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra
WWW.

Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

Odpowiedź:

Oferent zaproponował zapisy tożsame z już istniejącymi w opublikowanym OPZ. Oferent zaproponował zmniejszenie puli sygnatur ataków IPS z 5 tyś do 1 tyś., Zamawiający nie zgadza się na zamieszenie wymaganej puli. Zamawiający nie zgadza się do ograniczenia filtra WWW do 50 kategorii tematycznych, zamawiający pozostawia zapis w brzmieniu który w jego ocenie lepiej opisuje wymóg dotyczący minimalnej puli dostępnych sygnatur:
„Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora."

Jeżeli Oferent znajduje zapisy dyskryminujące jego ofertę prosimy o wskazanie ich wraz z uzasadnieniem.

Propozycja 12:

System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu

Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP

Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych

Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.

Odpowiedź:

Zamawiający określił wymagania w tym zakresie w sekcji „Uwierzytelnianie użytkowników w ramach sesji" w OPZ. Zamawiaj nie zgadza się na zmianę OPZ w tym zakresie. Jeżeli Oferent znajduje zapisy dyskryminujące jego ofertę prosimy o wskazanie ich wraz z uzasadnieniem.

Propozycja 13:

Urządzenie musi:

-posiadać certyfikat Common Criteria

-posiadać certyfikat ICSA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE

Odpowiedź:

Zamawiający sprecyzował swoje wymogi co do certyfikacji rozwiązania w sposób szeroki i jednocześnie gwarantujący odpowiednią jakość. Zamawiający podtrzymuje zapisy OPZ.

Propozycja 14:

Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Odpowiedź:

W OPZ opublikowanym przez zamawiającego w sekcji „Zarządzanie" zamieszczone zostały tożsame zapisy.

Propozycja 15:

Wymaga się, aby dostawa obejmowała również:

Minimum 12-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia dostawy.

Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 12 miesięcy liczoną od dnia dostawy.

Odpowiedź:

W OPZ opublikowanym przez zamawiającego w sekcji „Gwarancja oraz wsparcie" zamawiający precyzyjnie określił swoje wymogi w tym zakresie. Zamawiający podtrzymuje zapisy OPZ.

Z poważaniem

Wojciech Grzeniewski
Sekretarz Gminy Michałowice