URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA PODLASKIEGO
15-888 BIAŁYSTOK
ul. Kardynała Stefana Wyszyńskiego 1

Białystok, 09 sierpnia 2021 r.

BZP.272.19.2021

Wykonawcy
(uczestnicy postępowania)

Zamawiający informuje, iż w postępowaniu o udzielenie zamówienia publicznego pn. **„Rozwój e-usług Województwa podlaskiego”„ nr BZP.272.19.2021** wpłynęło pytanie, którego treść wraz z odpowiedzią przekazuję poniżej:

Na Zamawiającym, zgodnie z przepisami ustawy Prawo Zamówień Publicznych, spoczywa obowiązek przygotowania i przeprowadzenia postępowania o udzielenia zamówienia w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców.

*Po analizie załączników „Załącznik nr 1 e do OPZ Firewall średni_MŁomża” oraz „Załącznik nr 1 f do OPZ Firewall mały” nie udało się nam znaleźć innego rozwiązania, które spełnia łącznie wszystkie punkty wskazanych załączników niż rozwiązania **SOPHOS**.*

Pytanie nr 1:

1. Prosimy Zamawiającego o dopuszczenie poniższych wymagań równoważności:Załącznik nr 1 e do OPZ Firewall średni_M Łomża:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa orazfunkcjonalności dodatkowe.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

- *Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch*

trybów: Router/NAT lub transparent.

- *System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet*

10/100/1000.

- *System realizujący funkcję Firewall musi dysponować minimum 4 interfejsami SFP+ (10 GbE)*
- *Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o*

standard 802.1Q.

- *W zakresie Firewall’a obsługa nie mniej niż 1 000 000 jednoczesnych połączeń oraz 45 000 nowych*

połączeń na sekundę.

- *System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 200 GB do celów logowania i raportowania.*
- *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 logowaniaw postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.*
- *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*
    - *Analiza ruchu szyfrowanego protokołem SSL*
- *Wydajność systemu Firewall minimum 14 Gbps*
- *Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus*

minimum 2 Gbps

- *Wydajność ochrony przed atakami (IPS) minimum 7,5 Gbps*
- *Wydajność VPN IPSec, nie mniej niż 2 Gbps*
- *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 ssl vpn w trybach portal oraz tunel*
- *Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu oprotokoły: RIPv2, OSPF, BGP.*
- *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 protokołówdziałających 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.*
- *Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, niebazując jedynie na wartościach portów TCP/UDP.*
- *Baza filtra WWW pogrupowana w minimum 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 doglobalnej bazy zasilającej filtr URL.*
- *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*
- *W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jestnie 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 wymagaćdodatkowej licencji do swojego działania*
- *Urządzenie musi:*

-posiadać certyfikat Common Criteria EAL4+

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

- *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.*
- *Wymaga się, aby dostawa obejmowała również:*
- *Minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.*
- *Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.*

Odpowiedź:

Zmawiający akceptuje wymagania zaproponowane przez Wykonawcę.

Załącznik nr 1 f do OPZ Firewall mały:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa orazfunkcjonalności dodatkowe.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

- *Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóchtrybów: Router/NAT lub transparent.*
- *System realizujący funkcję Firewall musi dysponować minimum 12 interfejsami miedzianymi Ethernet10/100/1000.*
- *Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard*

802.1Q.

- *W zakresie Firewall'a obsługa nie mniej niż 500 tys jednoczesnych połączeń oraz 15 tys. nowych*

połączeńna sekundę.

- *System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 200 GB do celów logowania i raportowania.*
- *System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.*
- *Musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.*
- *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*
    - *Analiza ruchu szyfrowanego protokołem SSL*
- *Wydajność systemu Firewall min. 7 Gbps*
- *Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 800 Mbps*
- *Wydajność ochrony przed atakami (IPS) min 3,1 Gbps*
- *Wydajność VPN IPSec, nie mniej niż 1, Gbps*
- *Liczba tuneli IPSec VPN, nie mniej niż 450*
- *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*
- *Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.*
- *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 protokołówdziałających 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 minimum 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 doglobalnej bazy zasilającej filtr URL.*
- *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 nakontrolerze domeny*
- *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 wymagaćdodatkowej licencji do swojego działania*
- *Urządzenie musi:*

    -posiadać certyfikat Common Criteria EAL4+

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

- *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.*
- *Wymaga się, aby dostawa obejmowała również:*
- *Minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.*
- *Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.*

Odpowiedź:

Zmawiający akceptuje wymagania zaproponowane przez Wykonawcę.

W przypadku rozbieżności pomiędzy treścią SWZ, a treścią udzielonych wyjaśnień lub zmian SWZ, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

Zamawiający informuje, iż zostanie przedłużony termin składania ofert. Po opublikowaniu zmiany Ogłoszenia w Dzienniku Urzędowym Unii Europejskiej, zamawiający poinformuje o nowym terminie składania ofert.

z up. MARSZAŁKA WOJEWÓDZTWA

Marian Malinowski

Dyrektor Biura Zamówień Publicznych

/podpisano elektronicznie/