**

Załącznik do oferty

Załącznik nr 1D

Minimalne parametry techniczne i funkcjonalne

Firewall

|  |  |  |
| --- | --- | --- |
| **Szczegółowy opis** | | **Parametry oferowane** |
| **Lp.** | **Nazwa komponentu**  **Wymagane minimalne parametry** | **Spełnienie wymagań.**  **Spełnia /nie spełnia**  **(wypełnia Wykonawca)** |
|  | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności 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 min. 8 interfejsami miedzianymi Ethernet 10/100/1000. * Możliwość tworzenia min. 64 interfejsów wirtualnych definiowanych jako VLAN w oparciu o standard 802.1Q. * W zakresie Firewall obsługa nie mniej niż 300 tys. jednoczesnych połączeń oraz min. 18 tys. nowych połączeń na sekundę. * System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. * System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 64 GB lub pozwalać na zbieranie logów na zewnętrznym dysku, pendrive lub karcie SD o pojemności co najmniej 64 GB do celów logowania i raportowania. * 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 – komercyjny 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. 4 Gbps * Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 490 Mbps * Wydajność ochrony przed atakami (IPS) min. 2,4 Gbps * Wydajność VPN IPSec, nie mniej niż 600 Mbps * 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 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 minimum 65 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. * 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 * 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 * System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku, kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów * 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. | Nazwa  ........................ |

**Uwaga:**

**Wykonawca wypełnia kolumnę „Parametry i Spełnienie Wymagań”, podając informację czy proponowany system spełnia określone przez Zamawiającego minimalne parametry funkcjonalne oprogramowania poprzez użycie wyrazu „spełnia” lub „nie spełnia”.**

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.