**AE/ZP-27-10/22 ZAŁĄCZNIK NR 4**

##### Wymagane i oferowane parametry techniczne urządzenia UTM.

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **OPIS PARAMETRÓW URZĄDZENIA UTM** | **Wymagana  wartość.**  **Punktacja w kryterium „parametry techniczne”** | **Oferowana  wartość** |
|  | Polski interfejs użytkownika | TAK/NIE Podać  Punktacja:  Tak 10 pkt  Nie 0 pkt |  |
|  | Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. | Tak |  |
|  | Odrębny obraz maszyny wirtualnej tego samego producenta co system firewall w celu zbierania logów | TAK / NIE Podać Punktacja:  Tak 10 pkt  Nie 0 pkt |  |
|  | System realizujący funkcję Firewall musi dysponować minimum 12 interfejsami miedzianymi Ethernet 10/100/1000. | Tak |  |
|  | Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. | Tak |  |
|  | W zakresie Firewall’a obsługa co najmniej 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę. | Tak |  |
|  | System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 100 GB do celów logowania i raportowania. | Tak, Podać  Punktacja:  Pojemność  poniżej 150 GB – 0 pkt  Pojemność 150GB i więcej -10 pkt |  |
|  | System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. | Tak |  |
|  | Wraz z systemem bezpieczeństwa musi zostać dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. | Tak |  |
|  | 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 | Tak |  |
|  | Wydajność systemu Firewall min. 7 Gbps | Tak |  |
|  | Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 900 Mbps | Tak |  |
|  | Wydajność ochrony przed atakami (IPS) min 3,1 Gbps | Tak |  |
|  | Wydajność VPN IPSec, nie mniej niż 1 Gbps | Tak |  |
|  | Liczba tuneli IPSec VPN, nie mniej niż 450 | Tak |  |
|  | 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 | Tak |  |
|  | Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. | Tak |  |
|  | Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. | Tak |  |
|  | 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). | Tak |  |
|  | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. | Tak |  |
|  | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). | Tak |  |
|  | 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. | Tak |  |
|  | Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | Tak |  |
|  | Baza filtra WWW pogrupowana w minimum 50 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. | Tak |  |
|  | Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. | Tak |  |
|  | 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 | Tak |  |
|  | 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 | Tak |  |
|  | System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania | Tak |  |
|  | Urządzenie musi:  - posiadać certyfikat Common Criteria EAL4+ lub znajdować się na liście producentów Cybersecurity made in Europe stworzonej przez ESCO we współpracy z ENISA  - posiadać certyfikat ICSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE | Tak |  |
|  | 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. | Tak |  |
|  | 60-miesięczna pełna gwarancja na dostarczone urządzenie UTM od dnia protokolarnego odbioru kompletnego przedmiotu zamówienia. Rękojmia na przedmiot zamówienia: od dnia protokolarnego odbioru kompletnego przedmiotu zamówienia na zasadach i w terminie określonym w Kodeksie Cywilnym oraz umowie. | Tak |  |