**Nr postępowania: 23 Z TP 21**

Załącznik nr 1 do SWZ

*Nazwa i adres Wykonawcy* ..............................

**Opis przedmiotu zamówienia**

**ZESTAWIENIE WYMAGANYCH PARAMETRÓW   
TECHNICZNO-UŻYTKOWYCH GRANICZNYCH   
PRZEDMIOTU ZAMÓWIENIA**

**System** **bezpieczeństwa zabezpieczającego styk z Internetem oraz sieć wewnętrzną wraz   
z oprogramowaniem CPV: 32400000-7.**

1. **Nazwa i typ dostarczanego urządzenia** *(podać)*: …………………………………
2. **Producent** *(podać)*: …..……………………………..

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. System bezpieczeństwa zostanie dostarczony w postaci redundantnej, klastra wysokiej dostępności, co najmniej active-passive.

Wykonawca oświadcza, że zapewnia możliwość rozbudowy samodzielnie przez Zamawiającego Sprzętu o typowe urządzenia stosowane w serwerach, zgodnie z wymaganiami producenta Sprzętu (np. karty rozszerzeń, dyski itp.) bez utraty uprawnień wynikających z rękojmi za wady Sprzętu oraz bez utraty prawa do korzystania z usług gwarancyjnych.

Dla elementów systemu bezpieczeństwa wykonawca zapewni poniższe funkcjonalności:

|  |  |  |
| --- | --- | --- |
| **Lp** | **Parametry** | **Parametr graniczny** |
| 1 | Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. | Tak |
| 2 | System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 10GbE (SFP+) | Tak |
| 3 | System realizujący funkcję Firewall musi umożliwiać rozszerzenie dostępnych interfejsów o minimum 4 interfejsy optyczne 1GbE (SFP) oraz 8 interfejsów miedzianych Ethernet 10/100/1000 | Tak |
| 4 | Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. | Tak |
| 5 | W zakresie Firewall’a obsługa nie mniej niż 1 700 000 jednoczesnych połączeń oraz 85 000 nowych połączeń na sekundę. | Tak |
| 6 | System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 500 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. | Tak |
| 7 | 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. | Tak |
| 8 | 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 | Tak |
| 9 | Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 3,5 Gbps | Tak |
| 10 | Wydajność ochrony przed atakami (IPS) minimum 17 Gbps | Tak |
| 11 | Wydajność VPN IPSec, nie mniej niż 7 Gbps | Tak |
| 12 | 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 |
| 13 | Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. | Tak |
| 14 | Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. | Tak |
| 15 | 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 |
| 16 | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. | Tak |
| 17 | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). | Tak |
| 18 | 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 |
| 19 | Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | Tak |
| 20 | Baza filtra WWW pogrupowana w min 65 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. | Tak |
| 21 | Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. | Tak |
| 22 | 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 |
| 23 | 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 |
| 24 | System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania | Tak |
| 25 | 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 | Tak |
| 26 | 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 | Tak |
| 27 | 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 |
| 28 | Wymaga się, aby dostawa obejmowała również:   * + Minimum 12-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.   + Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 12 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu. | Tak |

**Dodatkowo punktowane parametry:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp** | **Parametry** | **Parametr punktowany** | **Potwierdzenie parametru punktowanego** |
| 1 | System realizujący funkcję Firewall posiada minimum 8 interfejsami miedzianymi Ethernet 10/100/1000 | **Tak – 10 pkt**  **Nie – 0 pkt** - |  |
| 2 | System realizujący funkcję Firewall z możliwością rozbudowy o redundantny zasilacz sieciowy | **Tak – 10 pkt**  **Nie – 0 pkt** |  |
| 3 | Wydajność systemu Firewall minimum 40 Gbps | **Tak – 10 pkt**  **Nie – 0 pkt** |  |