***Załącznik nr 1.1. do SWZ***

**Opis przedmiotu zamówienia dla części zamówienia I – Dostawa zapory sieciowej**

|  | **Nazwa elementu, parametru lub cechy** | **Zapora sieciowa 2 szt.**  **(dwa takie same urządzenia tworzące klaster HA)** |
| --- | --- | --- |
| 1. | Ogólne | 1. Rozwiązanie typu Next Generation Firewall/UTM 2. System zabezpieczeń posiada: moduł zabezpieczeń Firewall, interfejs GUI, interfejs CLI 3. rozwiązanie oparte jest o dedykowane urządzenia typu appliance (sprzęt i oprogramowanie tego samego producenta) 4. Konfiguracja urządzenia musi być możliwa poprzez: port konsoli szeregowej, port zarządzania i port typu ethernet. 5. System zabezpieczeń jest skonfigurowany w oparciu o dwa takie same urządzenia mogące pracować w trybie active/passive |
| 2. | Wydajność | 1. Wydajność urządzenia modułu zabezpieczeń jest nie mniejsza niż 15 Gbps 2. Wydajność urządzenia modułu zabezpieczeń posiada możliwość terminowania połączeń VPN z wydajnością nie mniejszą niż 15 Gbps, 3. Wydajność urządzenia modułu IPS powinna być nie mniejsza niż 15 Gbps, 4. Wydajność urządzenia modułu zabezpieczeń obsługuje nie mniej niż 5 000 000 równoległych sesji, minimum 125 000 połączeń na sekundę |
| 3. | Opis polityk | 1. Polityka bezpieczeństwa firewall w zakresie kontroli ruchu sieciowego powinna uwzględniać kierunek przepływu pakietów, protokoły, usługi sieciowe, użytkowników i serwery usług, stan połączenia oraz dane aplikacyjne 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego w konfiguracji automatycznej lub statycznej 4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa takich jak np. DMZ, LAN, WAN. 5. Możliwe powinno być budowanie warstwowych polityk bezpieczeństwa poprzez połączenie ze sobą kilku innych polityk bezpieczeństwa. |
| 4. | Funkcjonalność VPN | 1. System powinien realizować funkcję bezpiecznych połączeń IPSec VPN typu site to site oraz client to site warstwy drugiej i trzeciej 2. Uwierzytelnianie połączeń VPN odbywa się za pomocą certyfikatów cyfrowych 3. Uwierzytelnia w połączeniach client to site odbywa się z użyciem haseł lub certyfikatów 4. Połączenie IPSec VPN chronione jest za pomocą algorytmów AES128, AES256, 3DES, MD5, SHA 5. System musi umożliwiać konfigurację połączeń typu SSL VPN 6. Producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem na urządzeniach z systemem operacyjnym Android, Windows |
| 5. | Funkcjonalność IPS | 1. System zabezpieczeń zawiera wbudowany moduł wykrywania i ochrony przed intruzami (IPS). Sygnatury ataków są regularnie dostarczane przez producenta zabezpieczeń. 2. Moduł IPS umożliwia łatwy wybór wykorzystywanych sygnatur z za pomocą takich parametrów jak: poziom zagrożenia ataku oraz prawdopodobieństwo fałszywych alarmów, producent oprogramowania, typ aplikacji 3. Moduł IPS umożliwia wykorzystanie własnych sygnatur 4. Moduł IPS posiada przygotowane przez producenta zalecane profile konfiguracyjne 5. Moduł IPS zapewnia podstawową ochronę serwerów WWW |
| 6. | Uwierzytelnianie | 1. System powinien umożliwiać tworzenie polityki bezpieczeństwa w oparciu o użytkowników lub grup użytkowników 2. System powinien umożliwiać integrację z zewnętrzną bazą danych użytkowników: LDAP, Active Directory oraz możliwość wykorzystania wbudowanej bazy LDAP |
| 7. | Zarządzanie | 1. Komunikacja z platformą centralnego zarządzania realizowana jest z wykorzystaniem szyfrowanych protokołów. 2. Transmisja danych pomiędzy konsolą administratora a systemem zarządzania wyposażona jest w mechanizmy uwierzytelniania. 3. Zarządzanie może się odbywać za pomocą dedykowanej konsoli graficznej działającej na systemie Windows. 4. Autoryzacja administratorów realizowana jest za pomocą haseł statycznych, dynamicznych lub certyfikatów cyfrowych. 5. Możliwość definiowania szczegółowych uprawnień administratorów, np. tylko odczyt logów lub zarządzanie użytkownikami. 6. System wyposażony jest w moduł raportowania oraz zbierania i analizy logów. |
| 8. | Dodatkowe funkcje systemu bezpieczeństwa | 1. System zabezpieczeń zawiera wbudowany moduł anty-malware. sygnatury są regularnie dostarczane przez producenta zabezpieczeń 2. System zabezpieczeń zawiera wbudowany moduł antySPAM. 3. System zabezpieczeń zawiera wbudowany moduł chroniący przed niechcianą komunikacją z serwerami typu C&C 4. System umożliwia zablokowanie komunikacji lub przekierowanie jej do zaufanego serwera za pomocą protokołu DNS 5. System zabezpieczeń zawiera wbudowany moduł filtrowania stron WWW 6. System zabezpieczeń zawiera wbudowany moduł umożliwiający analizę komunikacji zaszyfrowanej za pomocą protokołu SSL 7. System zabezpieczeń zawiera moduł chroniący przed nowymi zagrożeniami poprzez analizę pliku w bezpiecznym, izolowanym środowisku (detonacja plików, analiza behawioralna) 8. Moduł analizy behawioralnej umożliwia wskazanie, na jakich systemach operacyjnych zostanie wykonana analiza behawioralna 9. Analiza behawioralna wykonywana jest na poziomie emulowanego systemu operacyjnego 10. System zabezpieczeń zawiera moduł chroniący przed nowymi zagrożeniami poprzez usuwanie zawartości potencjalnie niebezpiecznej z dokumentów, pozostawiając te niestwarzające zagrożenia 11. Środowisko emulacji zagrożeń wspiera systemy Windows 8.1, 10 i 11 |
| 9. | Obudowa (hardware) | 1. Metalowa, wysokość maksymalnie 1U / Desktop 2. Urządzenie wyposażone w minimum 8 portów RJ-45 1 GbE, minimum 2 porty RJ-45 2.5 GbpE i/lub 10 GbE (dopuszczalne konwertery SFP/SFP+ na RJ45) 3. porty konsolowe minimum USB-C, RJ-45 4. dysk SSD o minimalnych rozmiarze 480 GB 5. zainstalowane minimum 32 GB pamięci RAM na potrzeby systemu |
| 10. | Wsparcie | 1. W systemie jest wgrana najnowsza aktualna wersja oprogramowania 2. System bezpieczeństwa jest dostarczony z zestawem licencji/subskrypcji pozwalających na realizację funkcjonalności przez okres 12 miesięcy 3. System bezpieczeństwa jest dostarczony ze wsparciem na okres 12 miesięcy wymiarze czasowym minimum 8x5. 4. W ramach zakupu klastra HA uwzględnia się także wdrożenie niniejszego rozwiązania |
| 11. | Zasilanie | 1. Zasilacz 90-250V AC, 50-60 Hz 2. Urządzenie umożliwia opcjonalne podłączenie redundantnego zasilacza |

|  |  |
| --- | --- |
| Producent i model: | Wypełnić: |
| **Wartość brutto za całość** | Wypełnić: |

***DOKUMENT NALEŻY PODPISAĆ KWALIFIKOWANYM***

***PODPISEM ELEKTRONICZNYM LUB PODPISEM ZAUFANYM***

***LUB PODPISEM OSOBISTYM***

Producent musi znajdować się w rankingu Gartner Magic Quadrant i Foresters Wave

(w części LEADERS)

jak poniżej

[Link do najnowszego zestawienia na stronie Gartner – ranking ‘Hybrid Mesh Firewall’](https://www.gartner.com/doc/reprints?id=1-2LMB9DG8&ct=250806&st=sb&_gl=1*141nkwr*_gcl_au*NTIzODAwOTk0LjE3NjM2OTIwODk.)



[Link do najnowszego zestawienia na stronie Forester – ranking ‘Enterprise Firewall Solutions’](https://reprints2.forrester.com/#/assets/2/171/RES181412/report)

