......................................................

/nazwa i adres firmy/

**AP-26-23d/24 Załącznik nr 1a do oferty**

**Oferta w zakresie zaoferowanego sprzętu i systemów**

Urządzenie NGFW w trybie HA służącego do transmisji danych cyfrowych wraz z rozbudową środowiska służące do analizowania logów sieciowych spełnia następujące wymagania:

|  |  |  |  |
| --- | --- | --- | --- |
| **NGFW (Firewall następnej generacji)** | | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | | | **Oferowany model: …………………………….**  **Producent: …………………………………….** |
| Interfejsy - wymagania ogólne | | Urządzenie realizujące funkcję Firewall musi dysponować minimum:   * 16 portami Gigabit Ethernet RJ-45, * 8 gniazdami SFP 1 Gbps, * 8 gniazdami SFP+ 10 Gbps, * 2 gniazdami QSFP+ 40 Gbps. |  |
| Wraz z dostarczonym urządzeniem Zamawiający wymaga dołączenia kompatybilnych:   * 16 wkładek światłowodowych SFP 1 Gbps, * 16 wkładek światłowodowych SFP+ 10 Gbps, * 4 wkładek światłowodowych QSFP+ 40 Gbps. |  |
| Urządzenie musi posiadać port konsoli oraz port USB z możliwością instalacji oprogramowania z pendrive. |  |
| Urządzenie musi być wyposażone w dwa zasilacze. |  |
| Dostarczone urządzenie musi pozwalać na zdefiniowanie min. 200 wirtualnych interfejsów. |  |
| Wydajność - wymagania ogólne | | Firewall musi obsługiwać nie mniej niż 8 000 000 jednoczesnych połączeń oraz 480 tys. nowych połączeń na sekundę |  |
| Firewall w ramach funkcji stateful musi mieć przepustowość nie mniejszą niż 80 Gbps dla pakietów 512 B. |  |
| Urządzenie musi posiadać przepustowość nie mniejszą niż 25 Gbps z włączoną funkcją kontroli aplikacji. |  |
| Urządzenie musi osiągać wydajność szyfrowania IPSec VPN nie mniejszą niż 46 Gbps. |  |
| Firewall musi posiadać wydajność skanowania ruchu minimum 12 Gbps dla ochrony przed atakami |  |
| Firewall musi osiągać wydajność skanowania ruchu minimum 7 Gbps w przypadku włączonych funkcji IPS, Antywirus oraz Application Control. |  |
| Firewall musi mieć wydajność minimalnie 10 Gbps w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http. |  |
| Funkcje systemu ochrony - Wymagania ogólne | | System musi być wyposażony w zaporę ogniową klasy Stateful Inspection. |  |
| System musi pozwalać na szyfrowane połączenie za pośrednictwem protokołów IPSec VPN oraz SSL VPN. |  |
| System musi posiadać ochronę przed malware dla protokołów SMTP, IMAP, POP3, HTTP, FTP, HTTPS. |  |
| System musi mieć funkcję ochrony przed atakami IPS (Intrusion Prevention System). |  |
| System musi posiadać funkcję kontroli stron WWW. |  |
| System musi posiadać funkcję Antyspam dla protokołów pocztowych. |  |
| System musi posiadać funkcje zarządzania pasmem. |  |
| System musi posiadać mechanizmy ochrony przed wyciekiem informacji poufnej. |  |
| System musi posiadać uwierzytelnianie dwuskładnikowe z wykorzystaniem tokenów sprzętowych lub programowych. Wykonawca powinien dostarczyć min. 2 tokeny sprzętowe lub programowe. |  |
| System musi posiadać funkcję analizy ruchu szyfrowanego protokołem SSH. |  |
| System musi posiadać funkcję analizy ruchu szyfrowanego protokołem SSL. |  |
| Funkcje firewall - Wymagania ogólne | | Polityki funkcji firewall muszą uwzględniać:   * adresy IP, * użytkowników, * rejestr zdarzeń, * aplikacje lub zbiory aplikacji, * reakcję zabezpieczeń, * usługi sieciowe, * protokoły. |  |
| Funkcja firewall musi zapewniać translację adresów NAT oraz PAT. |  |
| Funkcja firewall musi umożliwiać utworzenie stref bezpieczeństwa takich jak: LAN, WAN, DMZ. |  |
| Funkcja firewall musi integrować się z następującymi rozwiązaniami SDN:   * Microsoft Azure, * Google Cloud Platform, * OpenStack, * VMWare vCenter, * Anazon Web Services. |  |
| Funkcjonalność VPN - wymagania ogólne | | Funkcjonalność VPN musi umożwiać konfigurację połączeń IPSec VPN. |  |
| Funkcjonalność VPN musi obsługiwać m.in. mechanizmy IPSec NAT Traversal oraz Xauth. |  |
| Funkcjonalność VPN musi obsługiwać szyfrowanie protokołem AES z kluczem 128 oraz 256 bitów. |  |
| Funkcjonalność VPN musi pozwalać na tworzenie połączeń Site-to-Site oraz Client-to-Site. |  |
| Funkcjonalność VPN musi umożliwiać stałe monitorowanie stanu tuneli VPN oraz ich aktywności. |  |
| Funkcjonalność VPN musi umożliwiać wybór tunelu dynamicznego lub routingu statycznego. |  |
| Funkcjonalność VPN musi posiadać mechanizm split tunneling dla połączeń Client-to-Site. |  |
| Funkcjonalność VPN musi zapewniać komunikację z wykorzystaniem protokołu SSL VPN z wykorzystaniem technologii HTML 5. |  |
| Funkcjonalność VPN musi umożliwiać instalację klienta VPN w celu realizacji połączenia. |  |
| Routing – wymagania ogólne | | System musi mieć możliwość konfiguracji routingu statycznego oraz dynamicznego routingu z wykorzystaniem protokołów:   * BGP, * OSPF, * RIPv2, * PIM. |  |
| Funkcjonalność ochrony przed atakami Malware – wymagania ogólne | | System musi zapewniać możliwość zarządzania pasmem:   * dla poszczególnych aplikacji, * dla wybranych URL. |  |
| Firewall engine musi pozwalać na skanowanie ruchu sieciowego dla wybranych portów, w tym portów niestandardowych. |  |
| System musi umożliwiać skanowanie archiwów rar oraz zip. |  |
| System ochrony musi zawierać sygnatury chroniące urządzenia mobilne. |  |
| System musi umożliwiać komunikację z platformą typu Sandbox. Wykonawca musi dostarczyć platformę typu Sandbox oraz niezbędne licencje upoważniające do korzystania w chmurze ze wskazanego rozwiązania. |  |
| System musi umożliwiać usuwanie aktywnej zawartości plików MS Office oraz PDF bez konieczności blokowania transferu całych plików. |  |
| Funkcjonalność ochrony przed atakami – Wymagania ogólne | | System musi mieć funkcje ochrony IPS (Intrusion Prevention System) przed atakami na infrastrukturę sieciową. |  |
| Ochrona musi opierać się min. na analizie anomalii w protokołach sieciowych oraz analizie sygnaturowej. |  |
| System musi chronić aplikacje, które korzystają z niestandardowych portów sieciowych. |  |
| Baza ataków musi być aktualizowana automatycznie i powinna zawierać min. 5000 wpisów. |  |
| Administratorzy systemu muszą mieć możliwość definiowania sygnatur oraz wyjątków. |  |
| System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego. |  |
| System musi realizować ochronę przed atakami typu DoS oraz DDoS. |  |
| System musi posiadać mechanizmy ochrony przed atakami na aplikacje webowe oraz możliwość kontrolowania długości nagłówka. |  |
| System musi umożliwiać wykrywanie i blokowanie komunikacji do sieci botnet. |  |
| Funkcja kontroli aplikacji – wymagania ogólne | | System musi umożliwiać głęboką analizę pakietów w celu kontroli aplikacji. |  |
| Kontrola aplikacji musi zawierać min. 2000 sygnatur oraz musi być aktualizowana automatycznie zgonie ze zdefiniowanym harmonogramem. |  |
| System musi umożliwiać kontrolę aplikacji chmurowych z wyszczególnieniem m.in. pobierania oraz wysyłania plików. |  |
| System musi umożliwiać definiowanie wyjątków oraz sygnatur. |  |
| Funkcja filtrowania WWW – wymagania ogólne | | Część systemu odpowiedzialna za kontrolę WWW musi korzystać z bazy składającej się z min. 40 mln adresów URL. |  |
| Filtr WWW musi posiadać podział na kategorie takie jak m.in.:   * Malware, * Phishing, * Spam * Proxy. |  |
| Filtr WWW musi pozwalać na blokowanie stron zgodnie z ustawą antyhazardową. |  |
| Filtr WWW musi posiadać funkcję przeciwdziałającą pojawianiu się niechcianych treści w wynikach wyszukiwarek, w tym m.in. google. |  |
| Administrator usługi musi mieć możliwość zdefiniowania komunikatów, które wyświetlać się będą w momencie użycia modułu filtrowania. |  |
| System musi umożliwiać wskazanie kategorii lub adresów URL dla których nie będzie dokonywana inspekcja. |  |
| Uwierzytelnianie – wymagania ogólne | | Wdrożone rozwiązanie musi umożliwiać weryfikację tożsamości użytkowników z wykorzystaniem:   * haseł przechowywanych w lokalnej bazie, * haseł przechowywanych w bazach ldap, * haseł przechowywanych w zewnętrznych bazach danych. |  |
| Wdrożone rozwiązanie musi umożliwiać konfigurację uwierzytelniania dwuskładnikowego. |  |
| Wdrożone rozwiązanie musi umożliwiać integrację ze środowiskiem Active Directory. |  |
| System zarządzania – wymagania ogólne | | System bezpieczeństwa musi pozwalać na zarządzanie za pośrednictwem protokołów SSH oraz HTTPS. |  |
| System musi umożliwiać współpracę z dedykowanymi platformami centralnego zarządzania oraz monitorowania z wykorzystaniem szyfrowanych protokołów. |  |
| System musi pozwalać na współpracę z rozwiązaniami monitorowania za pośrednictwem protokołu SNMP. |  |
| System musi umożliwiać przekazywanie statystyk z wykorzystaniem protokołów sflow lub netflow. |  |
| System musi umożliwiać zarządzanie za pośrednictwem zewnętrznego API. |  |
| System Firewall musi mieć wbudowane narzędzia diagnostyczne takie jak:   * Ping, * Traceroute, * Podgląd pakietów, * Stan sesji firewall. |  |
| System zarządzania musi umożliwiać wykonywanie zmian za pośrednictwem GUI oraz CLI. Zmiany powinny zostać zapisane po zatwierdzeniu przez administratora. |  |
| Log Management – wymagania ogólne | | System bezpieczeństwa musi pozwalać na logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania Wykonawca musi dostarczyć komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. |  |
| System pełniący funkcje firewall musi zapewnić przekazywanie danych o:   * ruchu zaakceptowanym, * ruchu blokowanym, * zużyciu zasobów, * stanie pracy systemu, * aktywności administratorów. |  |
| System musi umożliwiać wysyłanie logów do wielu serwerów logowania. |  |
| System logowania musi obejmować wszystkie moduły sieciowe oraz wszystkie moduły bezpieczeństwa w ramach oferowanego systemu. |  |
| System musi mieć możliwość logowania do serwera SYSLOG. |  |
| Certyfikat – wymagania ogólne | | Wszystkie składowe oferowanego systemu powinny posiadać dla funkcji Firewall certyfikat EAL4 lub ICSA. |  |
| Licencja, serwis, gwarancja – wymagania ogólne | | W ramach systemu muszą zostać dostarczone licencje upoważniające do korzystania przez 36 miesięcy z aktualnych baz funkcji ochronnych producenta oraz serwisów. |  |
| Licencje powinny obejmować:   * IPS, * Antywirus wraz z ochroną urządzeń mobilnych, * Kontrola Aplikacji, * Sandbox, * Antyspam, * Filtrowanie WWW, * Bazy adresów IP oraz domen. |  |
| System musi być objęty 36 miesięczną gwarancją producenta. |  |
| Zamawiający musi mieć możliwość wsparcia technicznego w trybie 24/7. |  |
| **System agregacji logów** | **Wymagane minimalne parametry techniczne** |  |
| Wymagania ogólne | | System musi zostać udostępnione w postaci komercyjnej. |  |
| System musi działać w oparciu o środowisko wirtualne dostarczone w niniejszym postępowaniu. |  |
| System musi obsługiwać powierzchnię dyskową o pojemności min. 3 TB. |  |
| System musi składać się z centralnego systemu logowania, systemu raportowania oraz systemu korelacji danych. |  |
| System logowania i raportowania musi pozwalać na zarządzanie z wykorzystaniem protokołów HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania przy wykorzystaniu szyfrowanych protokołów. |  |
| Wdrożony system musi uwierzytelniać administratorów z wykorzystaniem:   * haseł przechowywanych w lokalnej bazie, * haseł przechowywanych w bazach ldap, * haseł przechowywanych w zewnętrznych bazach danych. |  |
| System musi pozwalać na konfigurację min. 4 administratorów. Dla każdego z administratorów musi istnieć możliwość określenia praw dostępu do logowanych informacji i raportów. |  |
| Wydajność - wymagania ogólne | | System musi obsługiwać min. 25 GB logów sieciowych na dobę. |  |
| System musi pozwalać na pobieranie logów z min. 1000 systemów. |  |
| Log Management – wymagania ogólne | | System musi umożliwiać podgląd logowanych zdarzeń w czasie rzeczywistym. |  |
| System musi umożliwiać przeglądanie logów historycznych. |  |
| System musi umożliwiać filtrowanie logów. |  |
| System musi umożliwiać generowanie raportów graficznych oraz tekstowych, które przedstawiać będą stan pracy urządzenia oraz informacje dotyczące statystyk ruchu sieciowego oraz zdarzeń bezpieczeństwa. |  |
| Raporty muszą obejmować m.in.:   * najczęściej wykrywane ataki, * najczęściej wykorzystywane aplikacje, * najczęściej odwiedzane strony WWW, * najaktywniejszych użytkowników, * listę krajów z którymi najczęściej nawiązywane są połączenia, * najczęściej wykorzystywane polityki Firewall, * informacje nt. połączeń IPSec. |  |
| System musi umożliwiać przesyłanie danych logowania do innych systemów przetwarzania danych. Przekazywane logi muszą posiadać mechanizmy filtrowania. |  |
| Oferowany system centralnego logowania musi posiadać komunikację z systemami bezpieczeństwa z wykorzystaniem co najmniej UDP oraz TCP. |  |
| System musi zapewniać cykliczny eksport danych logowania do zewnętrznego systemu w celu długoczasowego składowania. Logi muszą być eksportowane z wykorzystaniem m.in. protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
| Raporty analizowanych logów (funkcjonalność Security Event Management) – wymagania ogólne | | System musi umożliwiać generowanie raportów w formatach CSV oraz PDF. |  |
| System musi zapewniać uprzednio skonfigurowane zestawy raportów z możliwością ich modyfikacji przez administratora. |  |
| System musi umożliwiać tworzenie własnych raportów. |  |
| System musi umożliwiać generowanie raportów cyklicznych wysyłanych na wskazany adres e-mail. |  |
| Korelacja danych (funkcjonalność Security Information Management) – wymagania ogólne | | System musi umożliwiać korelację logów dla realizowanych procesów. |  |
| System musi umożliwiać konfigurację powiadomień w przypadku wystąpienia określonych zdarzeń bezpieczeństwa. |  |
| Korelacja danych musi być możliwa m.in. dla następujących kategorii zdarzeń:   * IPS, * e-mail, * traffic, * malware, * aplikacje sieciowe. |  |
| Licencja i wsparcie techniczne – wymagania ogólne | | Oferowany system musi być dostarczony na własność. Brak wykupienia licencji wsparcia technicznego nie może spowodować zablokowania funkcjonowania sytemu. |  |
| System musi być objęty 12 miesięczną gwarancją producenta. |  |
| Zamawiający musi mieć możliwość wsparcia technicznego w trybie 24/7. |  |

…………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis)*

*(Dokument musi być złożony pod rygorem nieważności*

*w formie elektronicznej opatrzony podpisem zaufanym/*

*osobistym/kwalifikowalnym podpisem elektronicznym)*