# **Załącznik nr 5 do SIWZ**

# **Kryterium oceny: parametry techniczne**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametry techniczne** | ***TAK / NIE*** | ***Punkty*** |
| **I** | ***Integracja rozwiązania Sandbox*** | | |
| 1. | Rozwiązanie typu "sandbox" musi mieć możliwość otrzymywania plików do analizy bezpośrednio z urządzeń firewall wykorzystywanych w infrastrukturze Zamawiającego (klaster FortiGate 1500D). |  | ***4*** |
| 2. | Rozwiązanie typu "sandbox" musi umożliwiać urządzeniom firewall będącym w infrastrukturze Zamawiającego (klaster FortiGate 1500D) na korzystanie z generowanej lokalnie przez "sandbox" bazy zagrożeń (tzw. local threat intelligence), w szczególności min. :  - bazy złośliwych adresów URL,  - bazy hashy plików uznanych za niebezpieczne przez rozwiązanie typu sandbox.  Udostępniane dane muszą umożliwiać wzbogacenie profili bezpieczeństwa w regułach firewall, min. :  - automatyczne blokowanie plików na poziomie funkcjonalności antywirusa,  - blokowanie złośliwych adresów URL na poziomie funkcjonalności Webfiltering.  Informacje o zagrożeniach muszą być dostępne i wykorzystywane na rozwiązaniu firewall posiadanym przez Zamawiającego min. po 3 minutach od czasu wykrycia przez rozwiązanie typu "sandbox". |  | ***4*** |
| II | ***Integracja systemu logowania i urządzeń firewall (Firewall i System Logowania)*** | | |
| 1. | Dostarczany system logowania musi umożliwiać integrację z posiadanym przez Zamawiającego klastrem urządzeń firewall (FortiGate 1500D), tak aby min:   * logi z urządzeń firewall mogły być wysyłane, analizowane i umożliwiały generowanie gotowych raportów na poziomie systemu logowania, * logi historyczne muszą być zaczytywane do konsoli administracyjnej urządzeń firewall (FortiGate 1500D) z dostarczanego systemu logowania, * logi z urządzeń firewall posiadanych przez Zamawiającego (FortiGate 1500D) mają mieć możliwość dostarczenia w formie szyfrowanej. |  | ***4*** |
| 2. | Dostarczane rozwiązanie firewall musi umożliwiać integrację z dotychczasowym rozwiązaniem firewall posiadanym przez Zamawiającego (klaster FortiGate 1500D) min. na poziomie:   * wyświetlania w WebUI topologii fizycznej architektury bezpieczeństwa rozwiązania (połączenia pomiędzy dostarczanym rozwiązaniem firewall a posiadanym przez Zamawiającego), * wyświetlania w WebUI topologii logicznej architektury bezpieczeństwa rozwiązania (połączenia pomiędzy dostarczanym rozwiązaniem firewall a posiadanym przez Zamawiającego z uwzględnieniem interfejsów), * wyświetlania danych na temat urządzeń połączonych do posiadanego klastra firewall na WebUI dostarczanego rozwiązania firewall w zakresie: * typ urządzenia, * interfejs zapory sieciowej na którym widoczne jest urządzenie, * adres MAC, * Hostname, * Ilość aktualnych sesji, * Ilość wysłanych/odebranych pakietów przez podłączone urządzenie w pakietach na sekundę, * Ilość wysłanych/odebranych danych przez urządzenie w bajtach. |  | ***4*** |
| III | ***Możliwość rozbudowy kontroli antywirusowej na urządzeniach firewall (Firewall)*** | | |
| 1. | **Kontrola antywirusowa na poziomie urządzenia firewall**   1. System powinien umożliwiać rozbudowę o licencje lub subskrybcje umozliwijące:   - zablokowanie ataków zanim zostaną dla nich przygotowane sygnatury w bazie producenta – funkcja virus outbreak,  - sprawdzanie plików w czasie rzeczywistym na podstawie reputacji w oparciu o funkcje skrótu.   1. System powinien umożliwiać rozbudowę w oparciu o licencje lub subskrybcje umożliwiające usuwanie podejrzanej zawartości plików PDF oraz Microsoft Office bez koniczności blokowania transferu całych plików. |  | ***4*** |
| IV | ***Funkcje systemu Firewall (Firewall)*** | | |
|  | 1. System powinien umożliwiać tworzenie wewnętrznych akcelerowanych sprzętowo połączeń pomiędzy wirtualnymi instancjami. 2. Wsparcie dla routingu i przesyłania strumieni multicast wewnątrz tuneli IPSec przy zachowaniu akceleracji sprzętowej. 3. Dostarczony Klient VPN umożliwia weryfikację stanu bezpieczeństwa stacji zdalnej. 4. Rozwiązanie musi zapewniać funkcję VTEP (VXLAN Tunnel End Point). 5. Przy rozpoznawaniu aplikacji oprócz sygnatur powinny być stosowane algorytmy behawioralne. 6. System musi współpracować z oprogramowaniem klienckim producenta umożliwiającym szczegółowe rozpoznanie i sprawdzenie stanu bezpieczeństwa stacji końcowej zarówno w sieci firmowej jak i po ustanowieniu połączeń VPN w trybie tunel. Rozpoznane urządzenia lub ich grupy powinny być możliwe do użycia jako argument w polityce firewall. |  | ***4*** |
| V | ***Funkcjonalność proxy (Firewall)*** | | |
|  | 1. System musi pracować, jako forward proxy dla protokołów http, https, ftp, socks.  2. System powinien umożliwiać manipulowanie nagłówkami (dodawanie, usuwanie), np. CLIENT-IP, X-FORWARDED-FOR.  3. System musi zapewnić możliwości działania, jako:  • proxy dedykowane (explicit proxy),  • proxy transparentne (transparent proxy),  • explicit i transparent jednocześnie.  4. System musi umożliwiać wyłączenie skanowania ruchu HTTPS dla konkretnych kategorii stron www, użytkowników, adresów źródłowych lub docelowych.  5. System musi posiadać możliwość tworzenia polityk per adres IP, zakresów adresów IP, nazwy użytkownika, przynależności do grupy Active Directory/LDAP/lokalnej bazy/RADIUS/certyfikat użytkownika, nagłówki http np. X-FORWARDED-FOR.  6. System musi wspierać mechanizmy uwierzytelnienia: basic, digest,ntlm,form, negotiate(kerberos).  7. System musi umożliwiać wysyłanie informacji do zewnętrznego systemu poprzez protokół ICAP w trybie request mode i responde mode.  8. System musi posiadać funkcję Safe Search – przeciwdziałającą pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo**.** |  | ***4*** |
| VI | ***Integracja z urządzeniami dostępowymi i WAN, sprawdzanie stacji końcowej (Firewall)*** | | |
|  | **1**. System musi zarządzać urządzeniami dostępowymi i WAN tego samego producenta z wykorzystaniem protokołu CAPWAP:  • Punkty dostępowe bezprzewodowe,  • Przełączniki, w tym PoE ,  • Rozszerzenia interfejsu WAN obsługujące połączenia LTE.  2. Sieci SSID, VLAN oraz instancje WAN powinny być widziane jako interfejsy tego samego systemu. |  | ***4*** |
| VII | ***SDN Connector – Integracja z rozwiązaniami SDN (Firewall)*** | | |
|  | 1. System powinien integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych w celu użycia tych informacji przy budowaniu polityki firewall.  • CISCO ACI,  • AWS,  • VMware NSX,  • Nuage Networks,  • Microsoft Azure. |  | ***4*** |
| VIII | ***Automatyczne zewnętrzne listy blokady (Firewall)*** | | |
|  | Zewnętrzne listy blokady  1. System powinien umożliwiać automatyczne i cykliczne pobieranie z zewnętrznego serwera HTTP plików z listami URL, rekordów DNS czy adresów IP , które mogą być użyte w filtrach URL, inspekcji SSL, filtrach DNS oraz politykach proxy. |  | ***4*** |

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

*(upełnomocniony(ieni) przedstawiciel(e) Wykonawcy)*