**Załącznik nr 3 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Wymagania ogólne**

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2. Element systemu realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.
4. W ramach postępowania wymaganym jest dostarczenie licencji wsparcia dla posiadanego przez Zamawiającego centralnego systemu logowania, raportowania i korelacji FortiAnalyzer-2000E 3 Year 24x7 FortiCare Contract.
5. W ramach postępowania wymaganym jest dostarczenie licencji FortiSandbox-1000D FortiCare plus FortiGuard Threat Intelligence (AV, IPS, Web Filtering, File Query and SandBox Engine Updates) dla posiadanego przez Zamawiającego systemu do analizy i wykrywania zaawansowanych i nieznanych zagrożeń Sandbox.

**Urządzenie firewall klasy UTM.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | ***Szczegółowy opis oferowanych parametrów***  ***(nie dopuszcza się używania zwrotów np. „jak wymagane” lub podobnych)*** |
| 1. | **Wsparcie dla IPv4 i IPv6** | System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall; * Ochrony w warstwie aplikacji; * Protokołów routingu dynamicznego. |  |
| 2. | **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall; 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej; 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych; 4. Monitoring stanu realizowanych połączeń VPN; 5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |  |
| 3. | **Interfejsy, Dysk, Zasilanie** | 1. System realizujący 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.  1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB; 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q; 3. System musi być wyposażony w zasilanie 2xAC. |  |
| 4. | **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 480 tyś. nowych połączeń na sekundę; 2. Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B; 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 25 Gbps; 4. Wydajność szyfrowania IPSec VPN nie mniej niż 46 Gbps; 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 12 Gbps; 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps; 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 10 Gbps. |  |
| 5. | **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection; 2. Kontrola Aplikacji; 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN; 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS; 5. Ochrona przed atakami - Intrusion Prevention System; 6. Kontrola stron WWW; 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3; 8. Zarządzanie pasmem (QoS, Traffic shaping); 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP); 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site; 11. Analiza ruchu szyfrowanego protokołem SSL; 12. Analiza ruchu szyfrowanego protokołem SSH. |  |
| 6. | **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń; 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu; * Dedykowany ALG (Application Level Gateway) dla protokołu SIP;   3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN;  4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu:   * Amazon Web Services (AWS); * Microsoft Azure; * Cisco ACI; * Google Cloud Platform (GCP); * OpenStack; * VMware vCenter (ESXi). |  |
| 7. | **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2; * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM); * Obsługa protokołu Diffie-Hellman grup 19 i 20; * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE; * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site; * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego; * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth; * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:   * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0; * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta; * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| 8. | **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego; * Policy Based Routingu; * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| 9. | **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu; 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji; 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| 10. | **Kontrola Antywirusowa** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021); 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR; 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android); 4. System musi współpracować z posiadaną przez Zamawiającego platformą typu Sandbox. W ramach postępowania muszą zostać dostarczone niezbędne licencje i serwisy do posiadanej platformy typu Sandbox; 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| 11. | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych; 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach; 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora; 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur; 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS; 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies; 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| 12. | **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP; 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora; 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików; 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P; 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| 13. | **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne; 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy; 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard; 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL; 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo; 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania; 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| 14. | **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych;   2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego;  3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| 15. | **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania; 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów; 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego; 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow; 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację; 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall; 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| 16. | **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do istniejącego systemu logowania i raportowania FortiAanalyzer; 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania; 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu; 4. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| 17. | **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. |  |
| 18. | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:   * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |  |
| 19. | **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |
| 20. | **Rozszerzone wsparcie serwisowe** | Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.  **Wykonawca zgodnie z rozdziałem XVII SWZ wraz z ofertą złoży dokumenty:**   * Certyfikat ISO 9001 podmiotu serwisującego. |  |

**Centralny system analizy logów i raportowania.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | ***Szczegółowy opis oferowanych parametrów***  ***(nie dopuszcza się używania zwrotów np. „jak wymagane” lub podobnych)*** |
| 1. | **Oświadczenie o posiadanym rozwiązaniu.** | FortiAnalyzer - FAZ-2000E, Numer seryjny: FL-2KET318000009 |  |
| 2. | **Gwarancja oraz wsparcie** | W ramach postępowania należy dostarczyć licencję FortiAnalyzer-2000E 3 Year 24x7 FortiCare Contract, odnawiającą kontrakt serwisowy oraz dostęp do aktualizacji oprogramowania.  Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia `w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |

**System zaawansowanej ochrony przed zagrożeniami klasy Sandbox.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | ***Szczegółowy opis oferowanych parametrów***  ***(nie dopuszcza się używania zwrotów np. „jak wymagane” lub podobnych)*** |
| 1. | **Oświadczenie o posiadanym rozwiązaniu.** | FortiSandbox - FSA-1000D, Numer seryjny: FSA1KD3A17000349 |  |
| 2. | **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta co najmniej do 02.04.2024 r, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |
| 3. | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje: FortiSandbox-1000D FortiCare plus FortiGuard Threat Intelligence (AV, IPS, Web Filtering, File Query and SandBox Engine Updates) - upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów co najmniej. Powinny one obejmować:   * AV, IPS, Web Filtering, File Query, aktualizacje silnika Sandbox na okres co najmniej 33 miesięcy, * Rozszerzenie licencji dla ochrony w oparciu o wersje systemów Windows 8 i 10. |  |