|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Opis wymagań** |
|  | Typ | Urządzenie UTM (Unified Threat Management) przeznaczone do rozbudowy zabezpieczeń logicznych. System bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
|  | Ilość | 1 szt. |
|  | Podstawowe funkcjonalności | * porty LAN 10/100/1000 x 6, * wejścia USB x 1, * port konsoli RJ45 x 1, * przepustowość Threat Protection: 900 Mb/s, * przepustowość firewall (1518/512/64 byte UDP) 10/10/7 Gbps, * przepustowość SSL-VPN 950Mbps, * liczba użytkowników SSL-VPN: 200, * ilość jednoczesnych sesji (TCP) 1.500.000, * wbudowana usługa IPsec Site to Site IPSec VPN, * funkcjonalności: firewall, VPN, antywirus, IPS (ochrona przed atakami), filtrowanie treści WWW, ochrona przed spamem, DLP (ochrona przed wyciekiem informacji poufnej), kontrola aplikacji, optymalizacja pasma, kontroler sieci bezprzewodowych, mocne uwierzytelnianie, automatyczne aktualizowanie produktów zapewniające maksymalną ochronę przed zaawansowanymi zagrożeniami, * system musi być wyposażony w zasilanie AC. |
|  | Funkcje bezpieczeństwa | * kontrola dostępu - zapora ogniowa klasy Stateful Inspection, * kontrola aplikacji:   + funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP,   + baza powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora,   + aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików,   + baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P,   + administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur, * poufność transmisji danych – połączenia szyfrowane IPSec VPN oraz SSL VPN, * ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. * ochrona przed atakami – Intrusion Prevention System:   + ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,   + system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach,   + baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora,   + administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur,   + system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS,   + 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. * kontrola stron WWW:   + moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne,   + 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,   + filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard,   + administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL,   + funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo,   + administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania, * kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, * zarządzanie pasmem (QoS, Traffic shaping), * mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), * analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2, * system musi umożliwiać konfigurację połączeń typu IPSec VPN oraz SSL VPN. |
|  | Zarządzanie | * 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, * komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów, * powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego, * system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow, * element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall, * element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
|  | Licencjonowanie | 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, analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy. |
|  | Gwarancja | System musi być objęty serwisem gwarancyjnym producenta przez okres 60 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. |