**Urządzenie zapora ogniowa (1 sztuka).**

|  |  |  |  |
| --- | --- | --- | --- |
| **l.p.** | **Wymagany Parametr techniczny** | **Parametr oferowany****(należy wypełnić)** | Pełna nazwa oferowanego urządzenia z wskazaniem producenta oraz modelu **(należy wypełnić)**  |
| **1** | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |  |
| **2** | Monitoring stanu realizowanych połączeń VPN. |  |
| **3** | System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. |  |
| **4** | System realizujący funkcję Firewall powinien dysponować minimum 5 portami Ethernet 10/100/1000 Base-TX |  |
| **5** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
2. Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP,
3. HTTPS
4. Poufność transmisji danych  - połączenia szyfrowane IPSec VPN oraz SSL VPN
5. Ochrona przed atakami  - Intrusion Prevention System
6. Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie
7. niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
8. Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
9. Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
10. Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
11. Możliwość analizy ruchu szyfrowanego protokołem SSL
12. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
 |   |