**ZADANIE A: Uruchomienie i podstawowa konfiguracja**

NUMER INSTRUKCJI   
(WEDŁUG LAB ROADMAP)

**011**

**IBM Proventia MX** **1004** jest przykładem sprzętowego **Firewall** dla **branch office** opartego o zminiaturyzowany komputer typu PC.

System operacyjny zainstalowany jest na wbudowanym HDD 2,5’’. Urządzenie posiada konsolę CLI opartą o RS232 – dostępną poprzez złącze RJ45 dostosowane do Cisco rollover. Standardowe wyjście PC jest mapowane na tą konsolę (pozwala to na rezygnację z użytkowania monitora).

2. Należy połączyć urządzenie okablowaniem **RJ45 Cisco rollover** do gniazda konsoli i portu **RS232**. Parametry połączenia konsoli: 9600 kbps, 8 bitów danych, brak kontroli parzystości, 1 bit stopu.

3. IBM Proventia pracuje pod kontrolą zmodyfikowanego systemu Linux. Posiada łącznie **4 interfejsy FastEthernet:** 2 dedykowane (Internal, External), 2 dodatkowe.

Do systemu została dodana nakładka zarządzająca funkcjonalnością firewall. Nakładka automatycznie uruchamia się po zakończeniu ładowania systemu i umożliwia podstawowe konfigurowanie (domena, interfejsy, dostęp przez HTTPS, dane logowania, czas systemowy, tryb pracy itp.). Pozostałe czynności są dokonywane poprzez HTTPS. Domyślne dane logowania: admin/admin.

**UWAGA**: W nakładce urządzenie konfigurowane jest jako bramka **warstwy 3** (opcja router) lub ingerujący w wyższe warstwy **mostek filtrujący treść** (opcja transparent). W zależności od tego wyboru w później użytkowanym interfejsie HTTPS udostępniana jest inna funkcjonalność.

4. W przypadku braku możliwości zalogowania (zmieniono dane logowania) należy przywrócić urządzenie do stanu fabrycznego - poprzez pełną odbudowę filesystemu i jego konfiguracji z obrazu zapasowego znajdującego się na HDD). W tym celu należy w programie boot-menu (Grub) wybrać opcję: Proventia MX1004 Restore System Backup zamiast Linux-up.

**UWAGA**: ze względu na obecność HDD w urządzeniu należy ograniczyć do niezbędnego minimum odcinanie zasilania w celu resetowania. Po odcięciu należy dodatkowo odczekać kilka sekund przed przywróceniem zasilania.

5. Po uruchomieniu system powinien być dostępny przez **HTTPS** pod adresem **192.168.123.123**.

Domyślne dane logowania: admin/admin (HTTPS + Java).

6. Należy użyć tego adresu w przeglądarce WWW (HTTPS) - wcześniej wylogowując CLI. Następnie należy zainstalować certyfikat, co uruchomi manager Proventia Network MultiFunction Security.

**UWAGA**: do poprawnego funkcjonowania pakietu konieczne jest zezwolenie na uruchamianie treści mieszanej Java (klas/apletów podpisanych i nie podpisanych). W tym celu należy użyć panelu konfiguracji Java na stacji PC: Java Control Panel, zakładka „Advanced”, lista „Security/Mixed code”, ustawienie: Disable verification.

**ZADANIE B:** **Konfigurowanie IBM Proventia Firewall**

Należy dokonać pełnego przeglądu menu konfiguracji IBM Proventia Firewall i przetestować wybrane ustawienia.