**PB1: Przeglądanie reguł standardowych:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika
2. System wyświetla listę zdefiniowanych przez administratora reguł:
   1. adres źródłowy
   2. adres docelowy
   3. port
   4. protokół
   5. kierunek
   6. akcja

**PB2: Przeglądanie reguł związanych ze sterowaniem:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika
2. System wyświetla listę zdefiniowanych przez administratora reguł:
   1. adres docelowy
   2. funkcja
   3. rejestr
   4. akcja

**PB3: Dodawanie reguły standardowej:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika.
2. Administrator tworzy nową regułę z następującymi parametrami:
   1. adres źródłowy
   2. adres docelowy
   3. port
   4. protokół
   5. kierunek
   6. akcja
3. Reguła zostaje przekazana na koniec listy reguł przez system.

Scenariusz alternatywny 1 - reguła istnieje:

1-2. Jak w scenariuszu głównym.

1. Reguła z podanymi parametrami już istnieje, więc jej kopia nie zostanie dodana.

Scenariusz alternatywny 2 - użytkownik nie ma uprawnień administratora:

1-2. Jak w scenariuszu głównym.

1. Reguła nie zostaje dodana, ponieważ użytkownik ma za małe uprawnienia.

**PB4: Dodawanie reguły związanej ze sterowaniem:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika.
2. Administrator tworzy nową regułę z następującymi parametrami:
   1. adres docelowy
   2. funkcja
   3. rejestr
   4. akcja
3. Reguła zostaje przekazana na koniec listy reguł przez system.

Scenariusz alternatywny 1 - reguła istnieje:

1-2. Jak w scenariuszu głównym.

1. Reguła z podanymi parametrami już istnieje, więc jej kopia nie zostanie dodana.

Scenariusz alternatywny 2 - użytkownik nie ma uprawnień administratora:

1-2. Jak w scenariuszu głównym.

1. Reguła nie zostaje dodana, ponieważ użytkownik ma za małe uprawnienia.

**PB5: Usuwanie reguły:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika
2. Administrator wybiera regułę, którą chce usunąć.
3. System usuwa regułę podaną regułę z listy.
4. Wszystkie reguły, które znajdowały się poniżej, zostają przesunięte o jedną pozycję w górę.

Scenariusz alternatywny - użytkownik nie ma uprawnień administratora:

1-2. Jak w scenariuszu głównym.

1. Reguła nie zostaje dodana, ponieważ użytkownik ma za małe uprawnienia.

**PB6: Modyfikowanie reguły:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika.
2. Administrator wybiera regułę, którą chce zmodyfikować i zmienia jej parametry:
   1. pozycję na liście
   2. parametry filtrowania

Scenariusz alternatywny - użytkownik nie ma uprawnień administratora:

1-2. Jak w scenariuszu głównym.

1. Reguła nie zostaje dodana, ponieważ użytkownik ma za małe uprawnienia.

**PB7: Analiza zdarzeń bezpieczeństwa:**

Aktorzy: administrator

Scenariusz główny:

1. System sprawdza tożsamość i uprawnienia użytkownika.
2. System pobiera listę logów i listę reguł.
3. Na podstawie obu list system tworzy analizę zdarzeń bezpieczeństwa.
4. System wyświetla użytkownikowi listę zdarzeń bezpieczeństwa zapory sieciowej.

Scenariusz alternatywny - użytkownik nie ma uprawnień administratora:

1-2. Jak w scenariuszu głównym.

1. Użytkownik ma za małe uprawnienia do przeglądania logów.

**FU1: Logowanie użytkownika:**

Aktorzy: użytkownik, serwer WWW

Scenariusz główny:

1. Użytkownikowi zostaje wyświetlony formularz do zalogowania się do systemu.
2. Użytkownik wypełnia formularz i przesyła do weryfikacji.
3. Użytkownik uzyskuje dostęp do panelu administratora.

Scenariusz poboczny - użytkownik nie podał poprawnych danych:

1-2. Jak w scenariuszu głównym.

1. Użytkownik nie uzyskuje dostępu do panelu administratora.

Scenariusz poboczny - użytkownik nie jest administratorem.

1-2. Jak w scenariuszu głównym.

1. Użytkownik nie uzyskuje pełnego dostępu do panelu administratora - może jedynie przeglądać reguły.

**FU2: Wyświetlenie aktualnej listy reguł na serwerze WWW:**

Aktorzy: administrator, serwer WWW

Scenariusz główny:

1. Administrator otwiera okno reguł na serwerze.
2. System pobiera listę reguł zapisanych w pliku konfiguracyjnym.
3. System wyświetla listę reguł administratorowi.

**FU3: Modyfikowanie listy reguł na serwerze WWW:**

Aktorzy: administrator, serwer WWW, firewall

Scenariusz główny:

1-3. Jak w FU2.

1. Administrator wybiera rodzaj reguły.
2. Administrator wprowadza modyfikacje listy reguł.
3. Zaktualizowana lista reguł zostaje zapisana w pliku.
4. Firewall zostaje poinformowany o zmianie przez serwer WWW.
5. Firewall ładuje zmiany.

**FU4: Analiza zapytań z serwera przez firewall:**

Aktorzy: firewall, komputer sterujący

Scenariusz główny:

1. Interfejs sieciowy firewalla przyjmuje pakiety sieciowe i umieszcza je w kolejce wejściowej.
2. Pakiety z kolejki wejściowej przekazywane są do analizy nagłówków pod kątem zgodności z regułami filtracji sieciowej.
3. Odebrane z serwera zapytanie następnie analizowane jest pod kątem zgodności z regułami filtracji zapytań do sterowania.
4. Przefiltrowane zapytanie jest wysyłane do komputera sterującego.

Scenariusz poboczny 1 - pakiet jest odrzucony na poziomie filtracji pakietów:

1-3. Jak w scenariuszu głównym

1. Pakiety zostają odrzucone.
2. Szczegóły zapisywane są do logów.
3. Do hosta źródłowego odsyłana jest informacja o odrzuceniu.

Scenariusz poboczny 2 - pakiet jest odrzucony na poziomie analizy zapytań:

1-4. Jak w scenariuszu głównym

1. Zapytanie zostają odrzucone.
2. Szczegóły zapisywane są do logów.
3. Do hosta źródłowego odsyłana jest informacja o odrzuceniu.

**FU5: Analiza zdarzeń:**

Aktorzy: administrator, serwer WWW

Scenariusz główny:

1. Administrator wyznacza okres analizy zdarzeń.
2. System pobiera logi z wyznaczonego okresu.
3. Na podstawie listy reguł i logów tworzony jest widok historii zdarzeń.
4. Historia zdarzeń wyświetlona jest administratorowi.

Scenariusz poboczny 1 - pakiet jest odrzucony na poziomie filtracji pakietów

1-3. Jak w scenariuszu głównym

1. Pakiety zostają odrzucone.
2. Szczegóły zapisywane są do logów.
3. Do hosta źródłowego odsyłana jest informacja o odrzuceniu.