Laboratorium 1

Wprowadzenie do zapór sieciowych NetDefend

1. Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z graficznym interfejsem użytkownika zastosowanym w zaporach sieciowych NetDefend firmy D-link. Ćwiczenie obejmuje przegląd możliwości zapory DFL-260, założenia konstrukcyjne interfejsu zarządzającego oraz sposób konfigurowania zapór sieciowych serii NetDefend.

2. Specyfikacja zapory sieciowej DFL-260

Zapora sieciowaDFL-260 to skuteczne, działające w czasie rzeczywistym zabezpieczenie przed różnymi zagrożeniami sieciowymi dla małych i średnich biur z maksymalnie 50 użytkownikami. To urządzenie biurkowe w standardowej obudowie jest wyposażone w system zapobiegania włamaniom (Intrusion Prevention System - IPS), bramę antywirusowa (AntiVirus - AV) i mechanizm filtrowania treści (Web Content Filtering - WCF), dzięki czemu za konkurencyjna cenę rozwiązuje problemy firm związane z bezpieczeństwem sieci. DFL-260 zawiera system wykrywania włamań i zapobiegania im (IDP/IPS), bramę antywirusowa (AV) i mechanizm filtrowania treści i adresów internetowych, co zapewnia doskonała ochronę z kontrola treści w warstwie 7.

Rys. 1. Zapora sieciowa DFL – 260

Rys. 2. Panel tylni zapory sieciowej

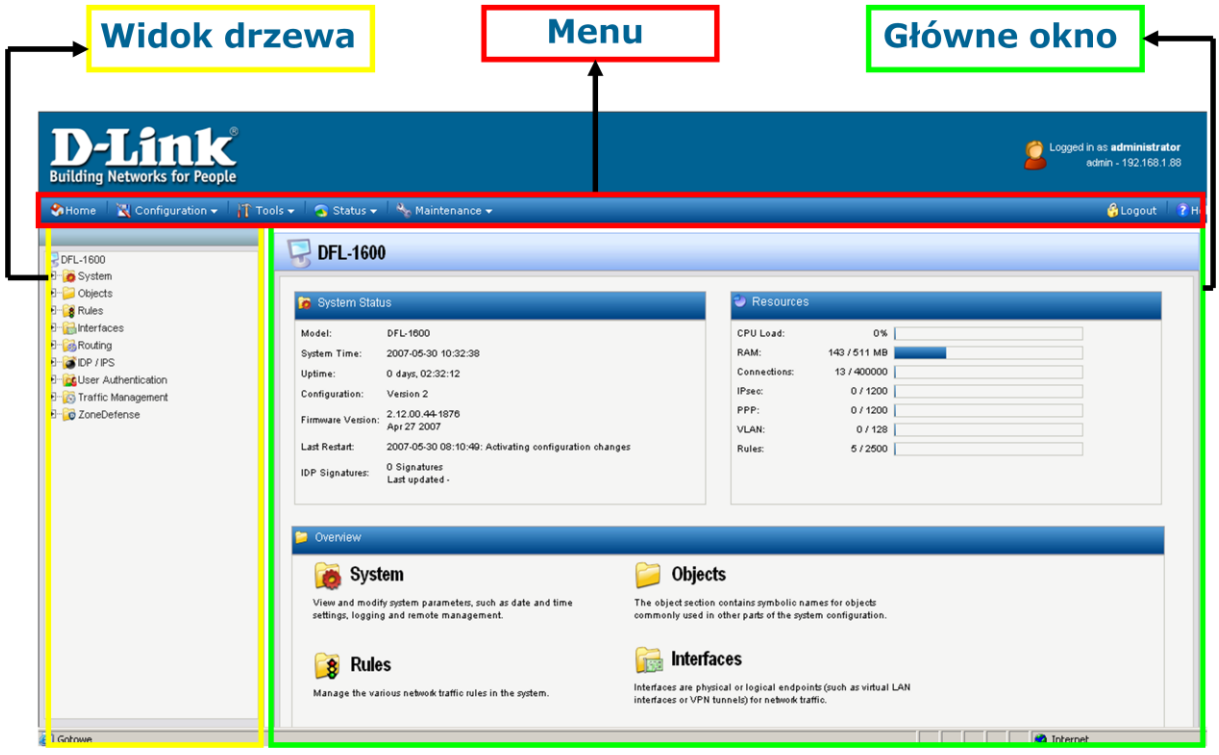
3. Podstawowa konfiguracja urządzenia

Domyślna konfiguracja zapory sieciowej DFL-260 zawiera trzy interfejsy zewnętrzne: WAN, DMZ oraz interfejs LAN. Domyślne ustawienia dla tych interfejsów przedstawiono w tabeli.

Tabela 1. Domyślna konfiguracja interfejsów – DFL-260

Wording on front plate	Default name in firewall	Default interface type definition	Default interface IP address	Default DHCP server status
WAN1	WAN1	DHCP Client	0.0.0.0	Disabled
DMZ	DMZ	Static IP	172.17.100.254/24	Disabled
Ports: 1-4	LAN	Static IP	192.168.1.1/24	Disabled

Adres interfejsu zarządzającego: https://192.168.1.1. Interfejs LAN umożliwia zarządzanie oraz odpowiada na ping. Serwer DHCP jest wyłączony
W celu uzyskania dostępu do graficznego interfejsu użytkownika należy skonfigurować statyczny adres IP (z podsieci 192.168.1.0/24) na maszynie zarządzającej a nastepnie wpisać w oknie przeglądarki adres https://192.168.1.1. Przed zalogowaniem użytkownik musi zostac uwierzytelniony. Należy zalogować się jako użytkownik: **admin** w pole hasła należy wpisać: **admin**. Interfejs użytkownika przedstawiono na Rys. 3.



3.1. Założenia koncepcyjne interfejsu zarządzającego

Reguły i foldery są przetwarzane po kolei w kolejności ich wystąpienia na liście - od pierwszej do ostatniej. Po kliknięciu prawym klawiszem na regule lub obiekcie i

wybraniu „**Delete**”, reguła lub obiekt zostaną zaznaczone do usunięcia i oznaczone przekreśleniem. Na takiej regule lub obiekcie można w ten sam sposób wykonać akcję „**Undo Delete**”. Po kliknięciu prawym klawiszem na regule lub obiekcie i wybraniu „**Disable**”, reguła lub obiekt zostaną dezaktywowane. Na takiej regule lub obiekcie można w ten sam sposób wykonać akcję „**Enable**”. Po wybraniu opcji „**Save** and **Activate**” nastąpi sprawdzenie konfiguracji i wyświetlenie błędów. Po kliknięciu „**Save and Activate**” użytkownik musi ponownie połączyć się z urządzeniem w domyślnym czasie 30 sekund aby ustawienia zostały zapisane (próba połączenia zostanie automatycznie podjęta po automatycznie ustalonym czasie). Jeśli takie połączenie nie nastąpi, urządzenie przywróci poprzednią, działającą konfigurację przy czym dokonane zmiany nie zostaną utracone. Domyślny czas 30 sekund może zostać zmieniony. Przy korzystaniu z interfejsu CLI, należy wydać polecenie „**activate**”, a następnie, po rekonfiguracji urządzenia - polecenie „**commit**”.

3.2. Kroki konfiguracyjne

Konfiguracja zapory sieciowej składa się z trzech głównych kroków:
Pierwszym krokiem jest utworzenie **OBIEKTU.** OBIEKT jest najważniejszym elementem w konfiguracji zapory sieciowej. OBIEKT jest podstawowym elementem zdefiniowanym w konfiguracji. OBIEKT jest nazwą symboliczną, do której przyporządkowane mogą być różne typy adresów z włączeniem adresów hostów oraz adresów sieci. Obiekty są silnie wykorzystywane w konfiguracji urządzenia – tablicy routingu, zestawie reguł, definicji interfejsów, tunelach VPN i innych. Zapory sieciowe NetDefend posiadają sześć rodzajów obiektów: Książkę adresową, Bramy warstwy aplikacyjnej, Usługi, Kalendarz, Uwierzytelnianie oraz VPN.
Następnym krokiem konfiguracji jest utworzenie **reguł**. Sekcja Reguły (Rules) jest „sercem” urządzenia. Zestaw reguł jest głównym filtrem pozwalającym na regulowanie przepływu pakietów przez zaporę sieciową. Reguły określają ponadto, jakie inne akcje należy na pakietach przeprowadzić (NAT/SAT).
Ostatnim krokiem konfiguracji jest utworzenie **tablicy routingu**. Główna trasa routingu (Main Route) Sekcja konfiguracyjna tras routingu opisuje tablicę routingu urządzenia. Trasa routingu na bazie polis (Policy-Based Route) Reguły w tablicy routingu na bazie polis (PBR) określają, której tablicy routingu użyć przy przekazywaniu pakietu w obydwie strony (priorytety routingu). Tablica routingu określa, w jakim kierunku powinny być wysłane pakiety przeznaczone dla określonej sieci docelowej (lub adresu IP). Jako pierwsza wybrana będzie trasa routingu o najdłuższym prefiksie (liczbie bitów w masce ustawionych na 1). Jeśli długość prefiksu sieci będzie taka sama, wybrana zostanie trasa routingu z niższą metryką. Jeśli metryki będą takie same, wybrana zostanie trasa routingu znajdująca się na wyższej pozycji w tablicy routingu. Zakładając, że istnieje tablica routingu:

192.168.20.16/28
192.168.0.0/16

Jeśli pakiet ma zostać wysłany do adresu 192.168.20.19, to obydwa wpisy w tablicy routingu wskazują lokalizację docelową. W tym wypadku zostanie wybrana trasa do sieci o dłuższym prefiksie (/28) jako lepiej pasująca (mająca więcej bitów w adresie docelowym zgodnych z adresem danej sieci).

4. Zadania do samodzielnego wykonania

4.1. Zapoznać się z graficznym interfejsem użytkownika zapory sieciowej DFL-260.
4.2. Utworzyć następujące obiekty w książce adresowej: DHCP_pool, Netmask, DNS1 i DNS2
4.3. Dodać serwer DHCP wykorzystując utworzone wcześniej obiekty z książki adresowej.
4.4. Zapisać i aktywować konfiguracje.
4.5. Wykonane kroki konfiguracyjne udokumentować