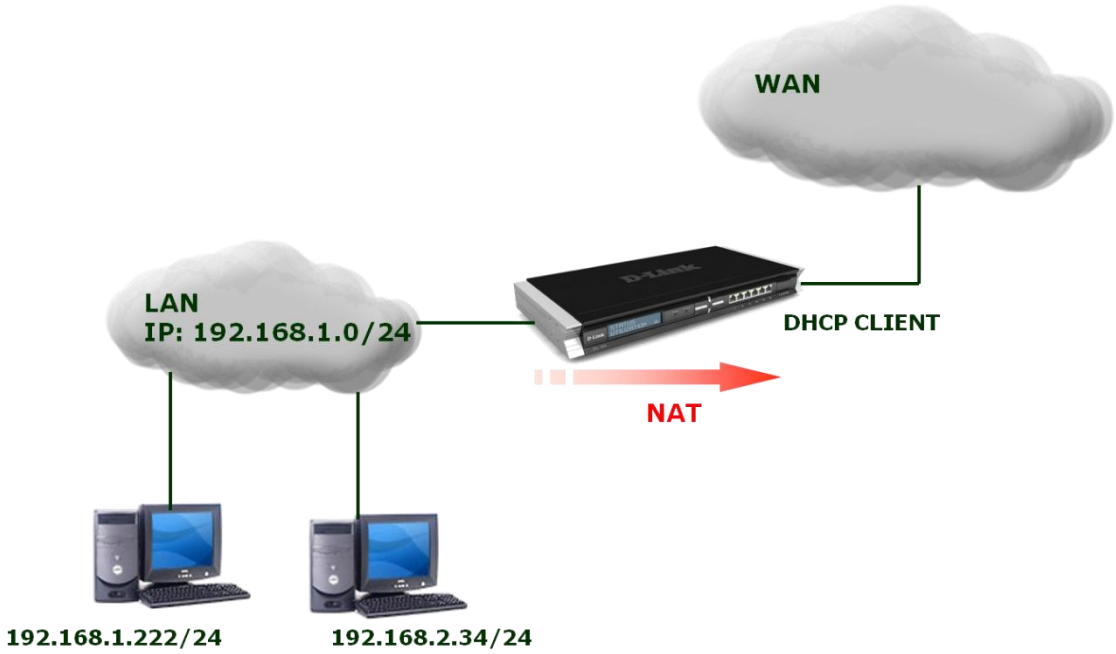
Laboratorium 2

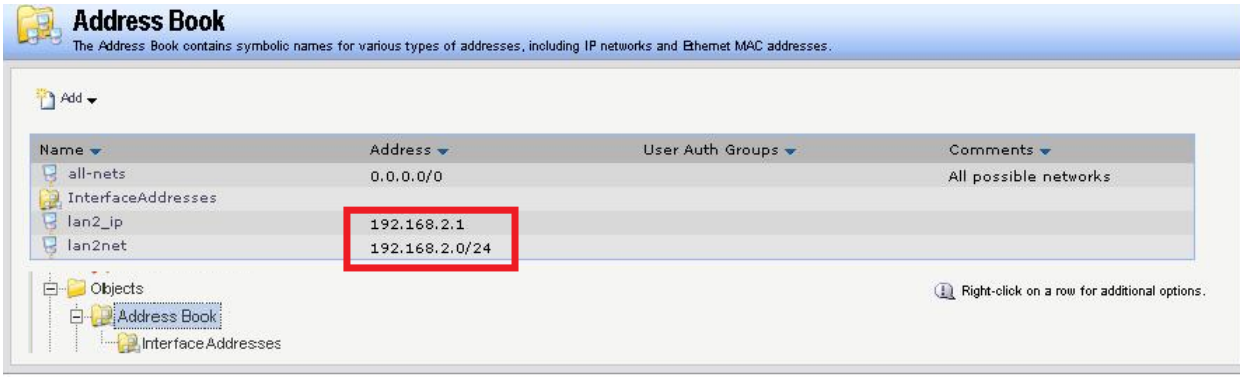
Zaawansowana konfiguracja i zarządzanie zaporami sieciowymi D-Link NetDefend cz.2.

1. „Druga” podsieć na interfejsie

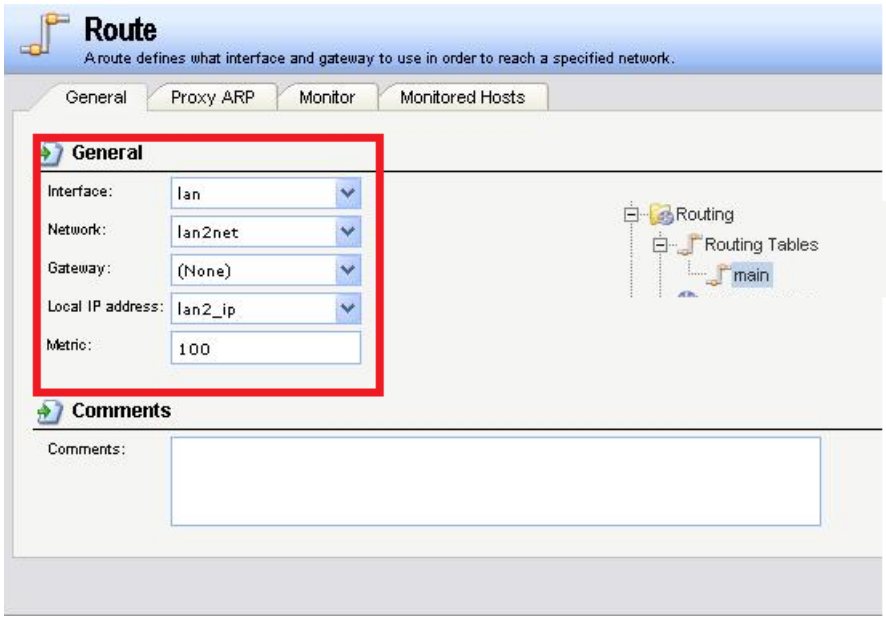


Na potrzeby ćwiczenia należy ustawić na komputerach ręcznie adresy IP jak na rysunku powyżej oraz ręcznie podać adresy serwerów DNS: DNS1: 157.158.3.1 DNS2: 157.158.3.2.

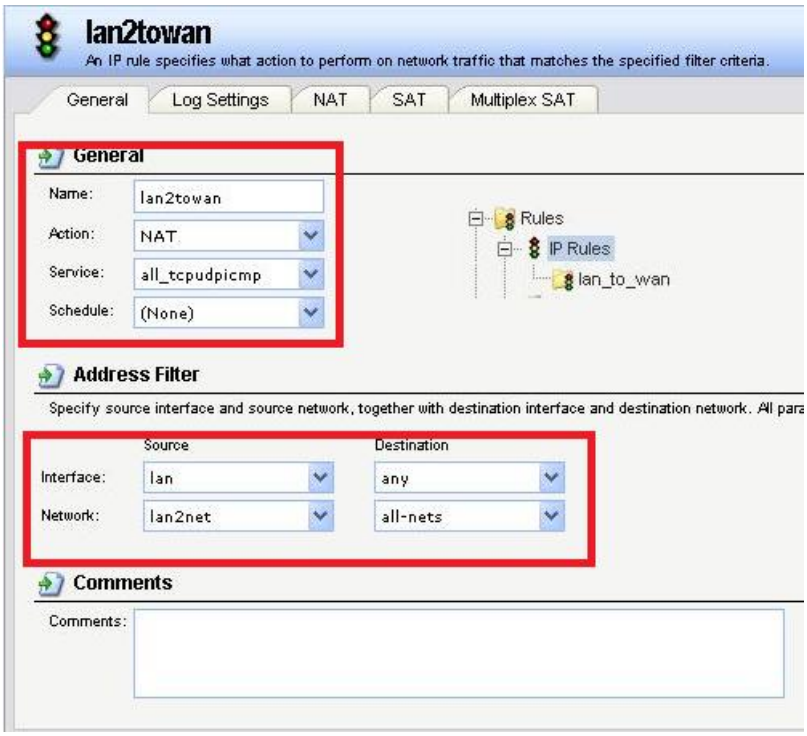
W książce adresowej utworzyć obiekty dla lokalnej podsieci i lokalnego adresu IP



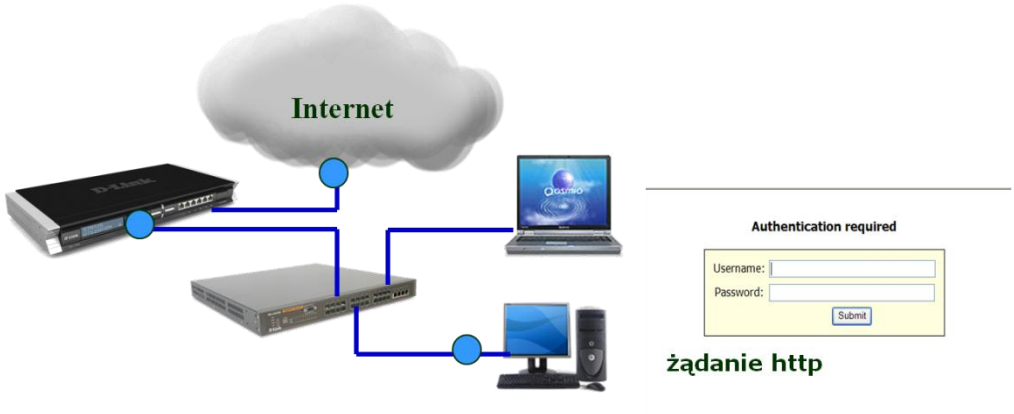
W głównej tablicy rutingu dodać trasę routingu do lokalnie przyłączonej sieci na interfejsie LAN. Wpisać jako *Local IP Address* adres, który ma zostać dodany na interfejsie zapory sieciowej jako adres lokalny.



Utworzyć regułę NAT maskującą ruch z „drugiej” podsieci do Internetu.



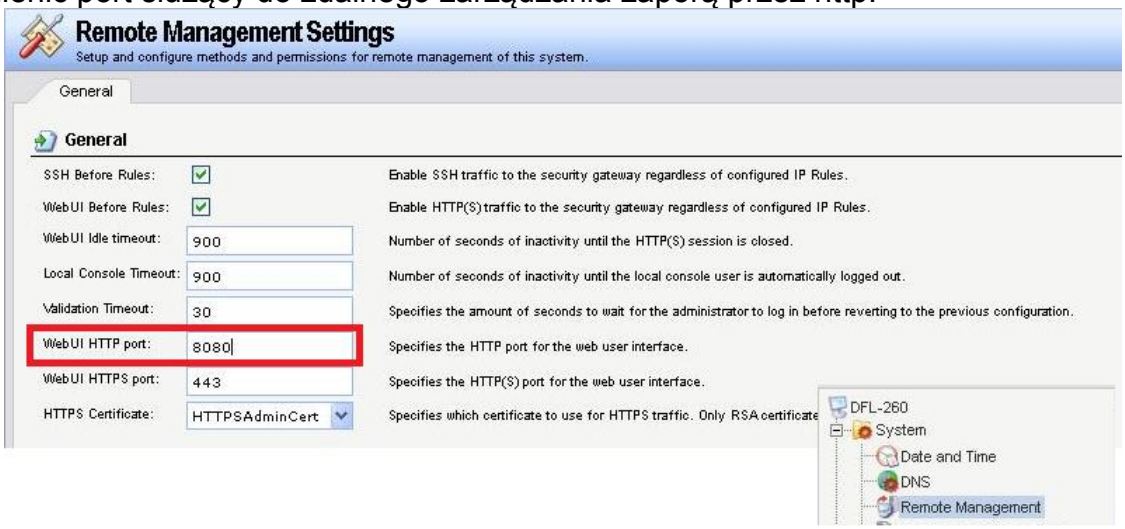
2. Uwierzytelnianie dostępu do Internetu



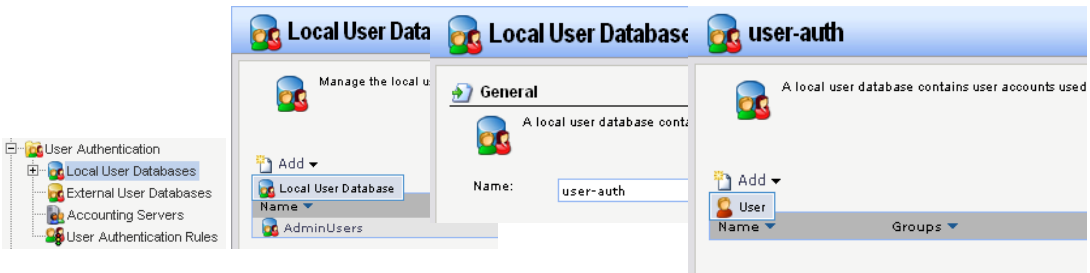
Dopuszczenie użytkownika do Internetu nastąpi po jego uwierzytelnieniu się poprzez podanie nazwy użytkownika i hasła na stronie logowania. Dane do uwierzytelniania mogą zostać pobrane z lokalnej bazy danych lub z serwera typu RADIUS. Wylogowanie może nastąpić ręcznie lub po upływie ustawionego czasu nieaktywności.

Na potrzeby ćwiczenia należy ustawić na komputerach ręcznie adresy IP z podsieci 192.168.1.0/24 oraz ręcznie podać adresy serwerów DNS: DNS1: 157.158.3.1 DNS2: 157.158.3.2.

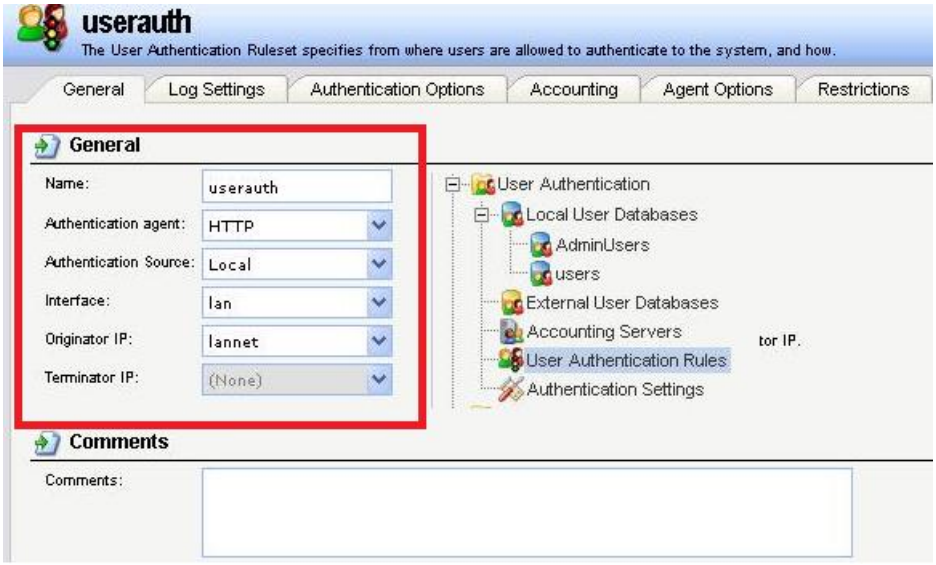
Zmienić port służący do zdalnego zarządzania zaporą przez http.



Utworzyć lokalną bazę danych użytkowników następnie dodać użytkownika oraz hasło.

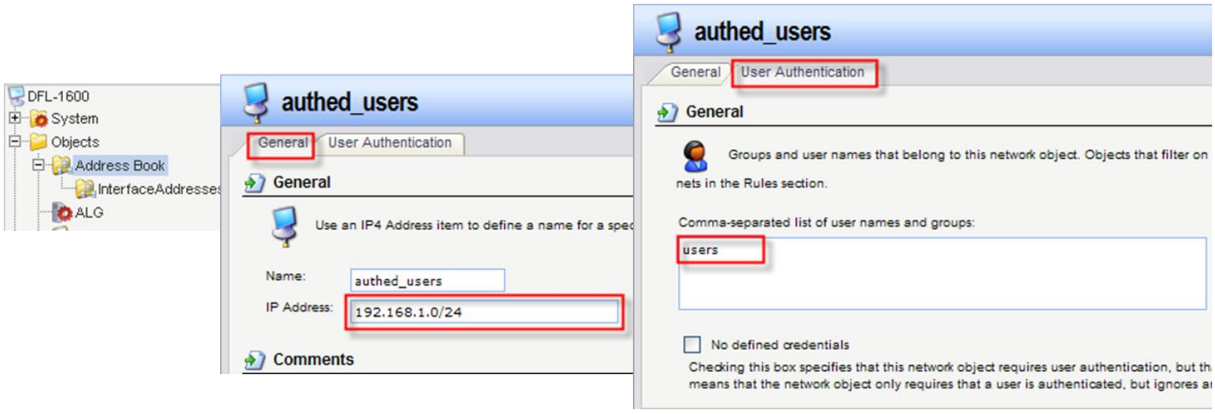


Utworzyć regułę uwierzytelniania użytkowników: wybrać agenta uwierzytelniania, rodzaj bazy danych, interfejs oraz podsięc do uwierzytelniania.

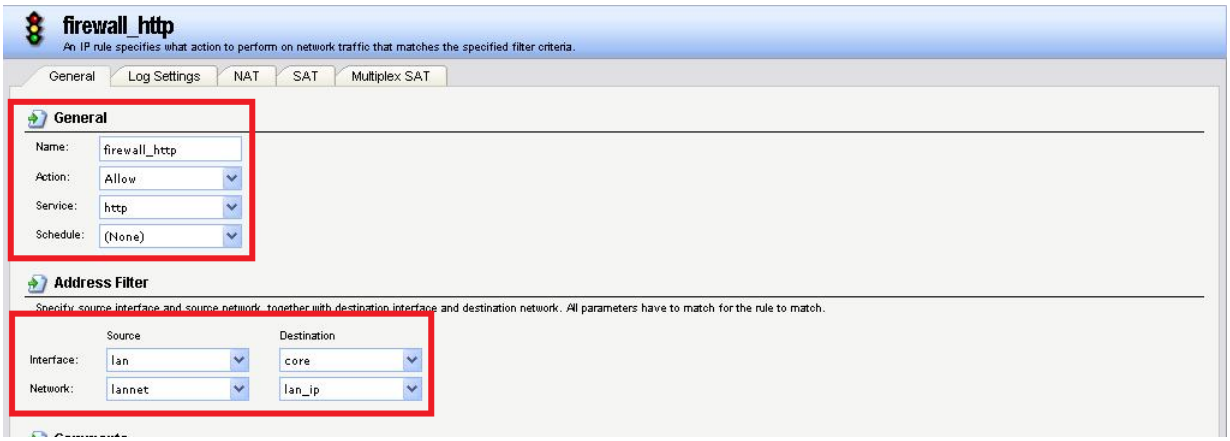


Wskazać bazę danych, z której mają być pobierane dane do procesu uwierzytelniania, oraz zdefiniować czasy po których nastąpi samoczynne wylogowanie.

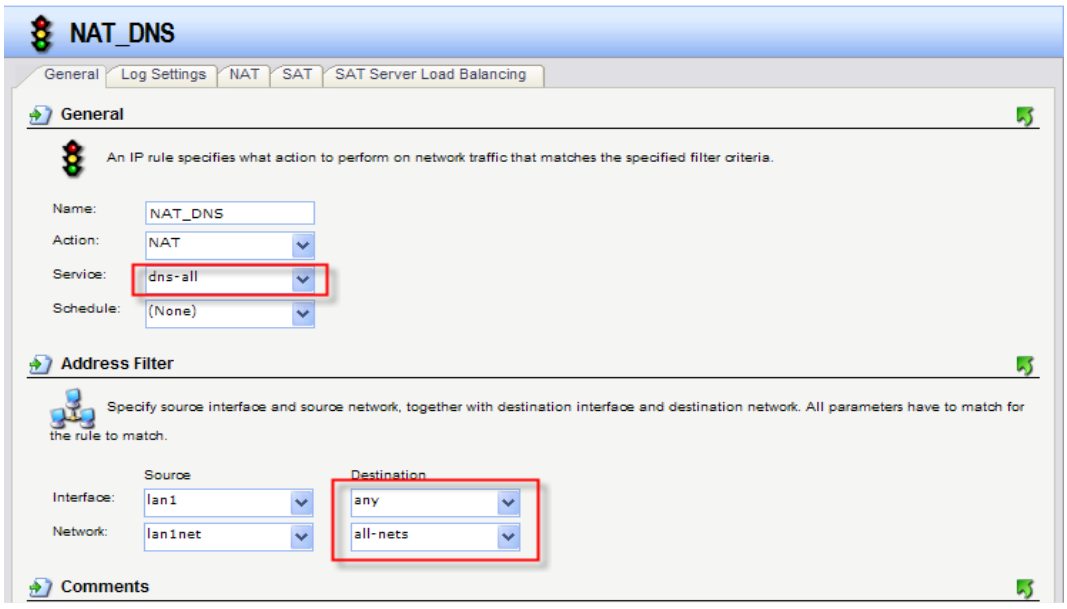
W książce adresowej utworzyć obiekt dla uwierzytelniania użytkowników. Wprowadzić grupę adresów IP oraz nazwę grupy użytkowników.



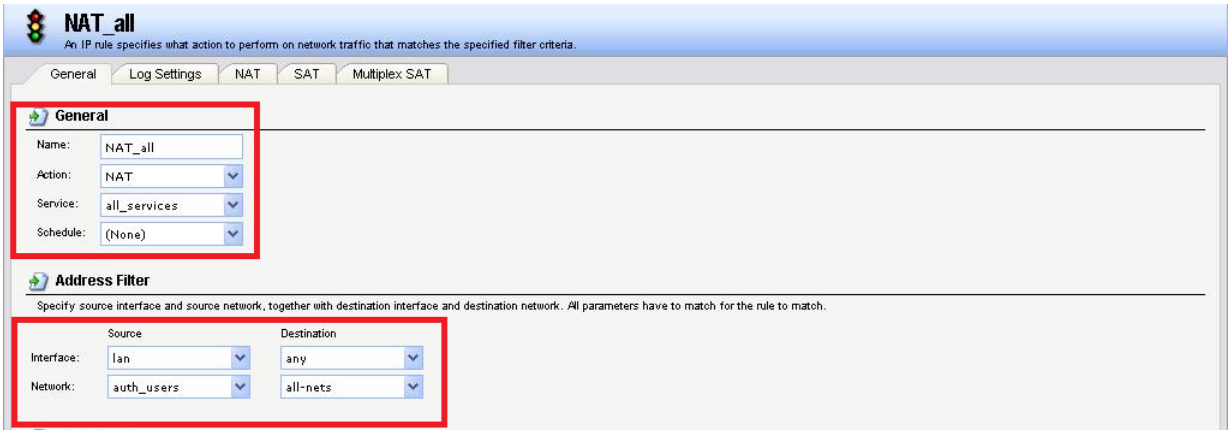
Usunąć istniejący reguły LAN to WAN. Utworzyć regułe IP (Allow – reguła nr. 1) zezwalającą na ruch http służący do uwierzytelniania i kierowany do interfejsu zarządzającego zapory sieciowej.



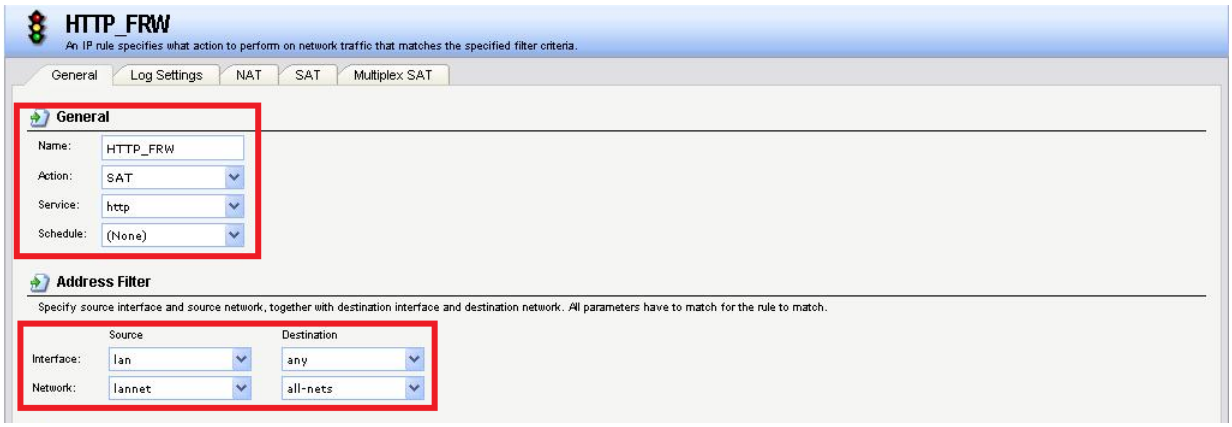
Utworzyć regułę IP (NAT – reguła nr. 2) zezwalająca na ruch do serwerów DNS.



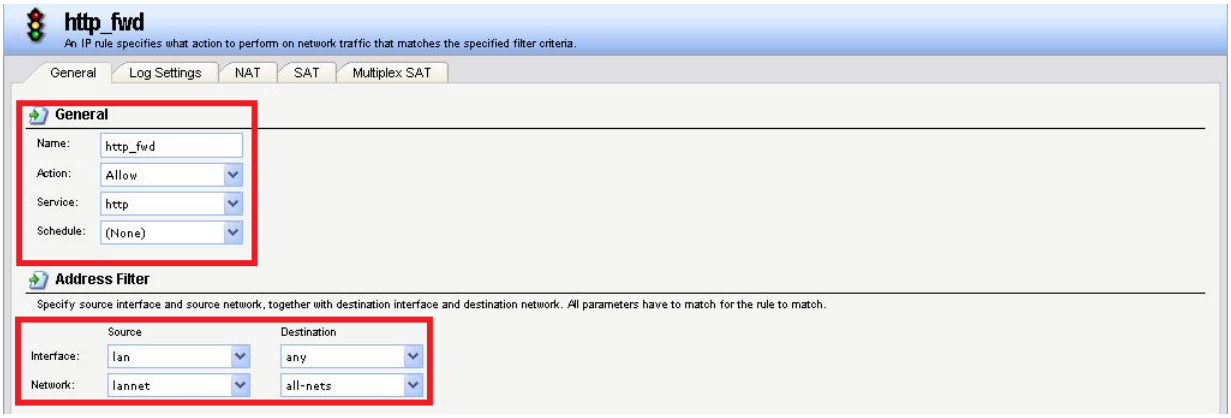
Utworzyć regułę IP (NAT – reguła nr. 3) zezwalająca na dowolny ruch dla użytkowników uwierzytelnionych.



Utworzyć regułę IP (SAT – reguła nr. 4) przekierowującą ruch http użytkowników nieuwierzytelnionych na stronę logowania.

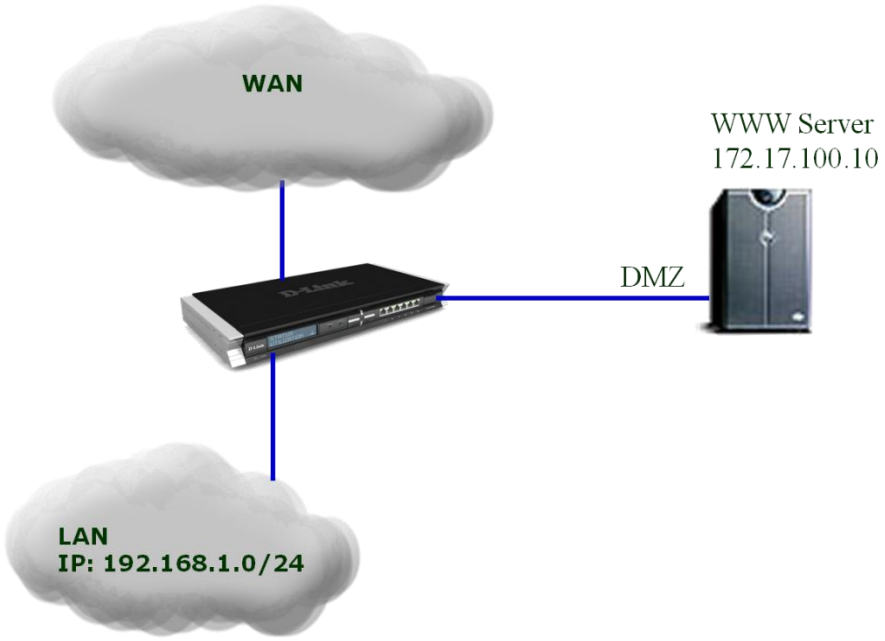


Utworzyć regułę IP (Allow – reguła nr. 5) przekierowująca ruch http użytkowników nieuwierzytelnionych na stronę logowania.



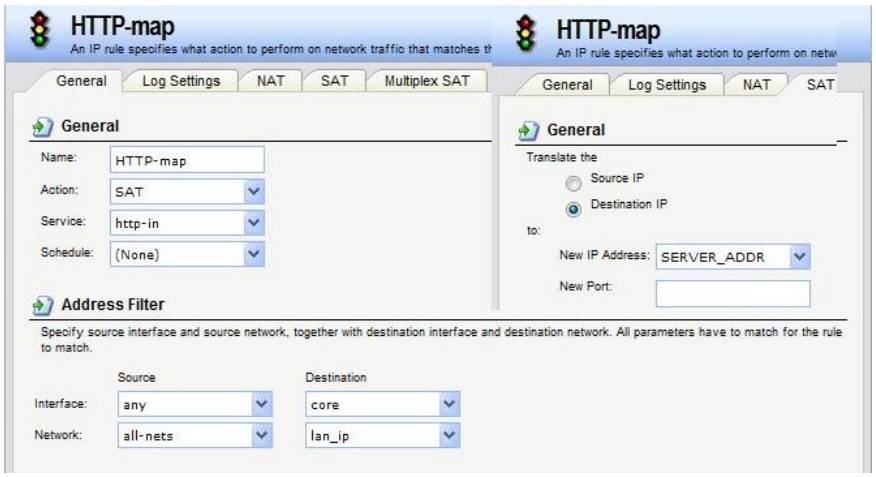
Zapisać i aktywować konfigurację.

3. Mapowanie portu (serwer wirtualny)

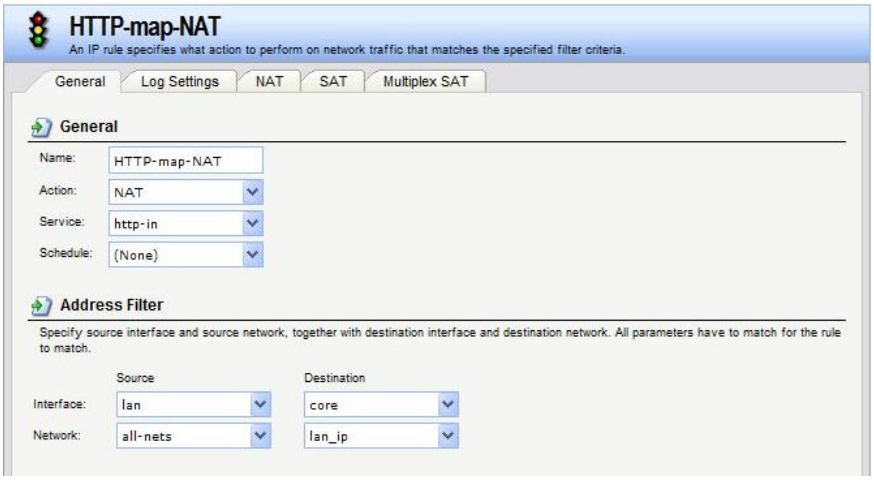


Na potrzebe ćwiczenia przywrócić ustawienia domyślne zapory. W książce adresowej dodać obiekt dla serwera WWW.

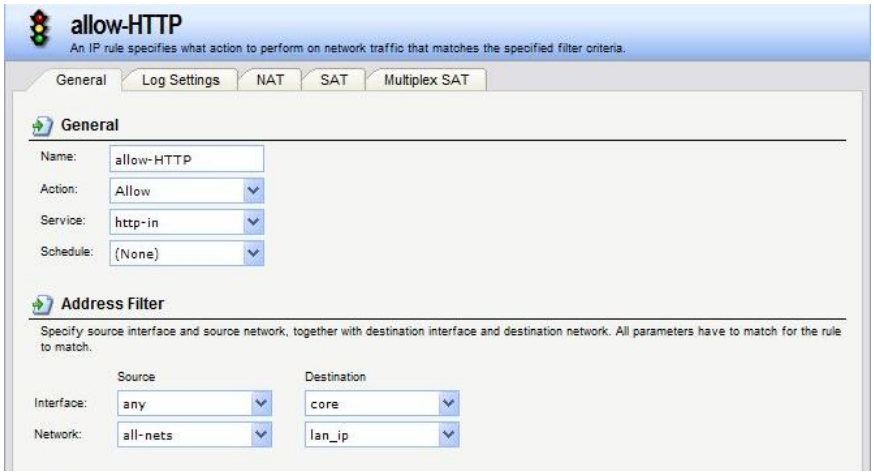
Utworzyć regułę IP wykonująca akcje SAT.



Utworzyć regułę IP wykonująca akcje NAT – aby umożliwić dostęp z sieci lokalnej przez adres publiczny do serwera.



Utworzyć regułę IP (Allow) zezwalająca na ruch do serwera WWW.



Zapisać i aktywować konfiguracje.