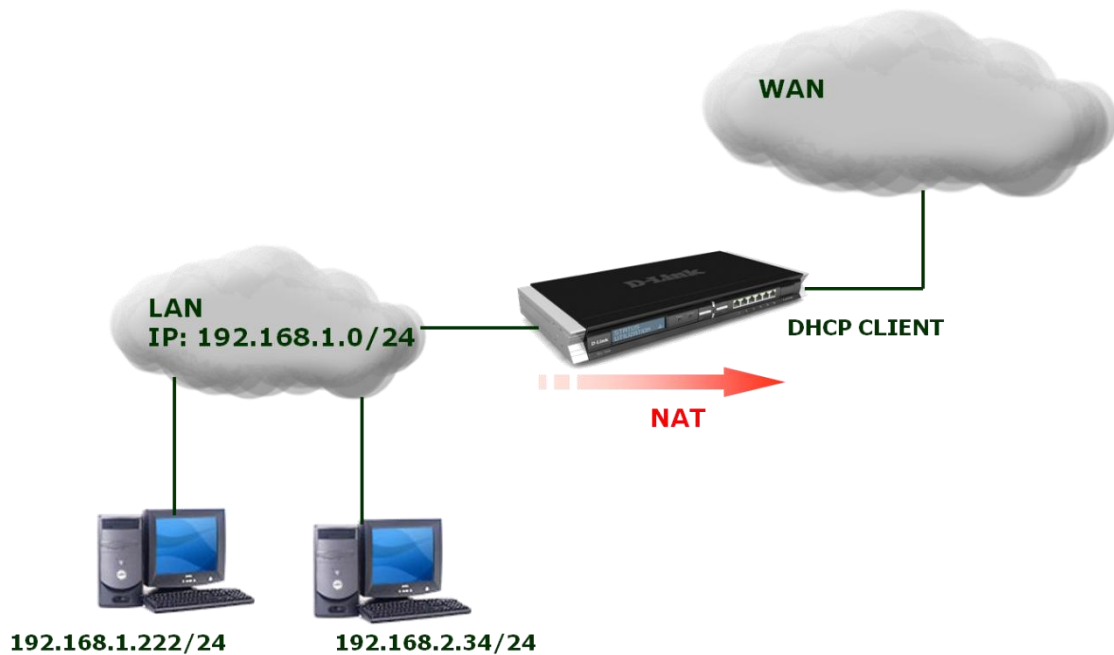


Laboratorium 2

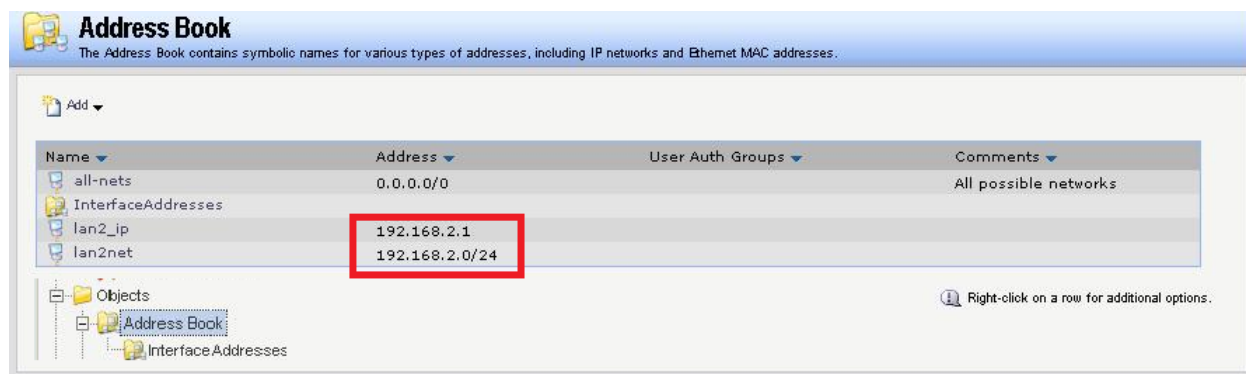
Zaawansowana konfiguracja i zarządzanie zaporami sieciowymi D-Link NetDefend cz.2.

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 routingu 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.

Route
A route defines what interface and gateway to use in order to reach a specified network.

General Proxy ARP Monitor Monitored Hosts

General

Interface:

Network:

Gateway:

Local IP address:

Metric:

Routing
Routing Tables
main

Comments

Comments:

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

lan2towan
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name:

Action:

Service:

Schedule:

Rules
IP Rules
lan_to_wan

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters are required.

Source Destination

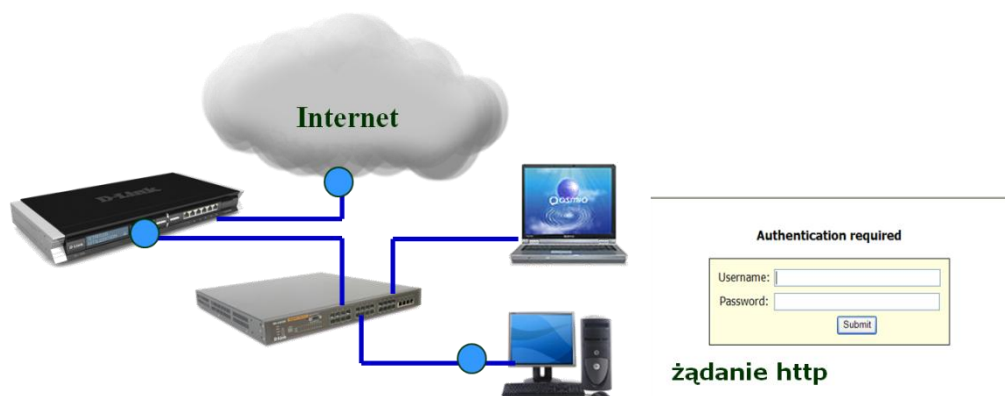
Interface:

Network:

Comments

Comments:

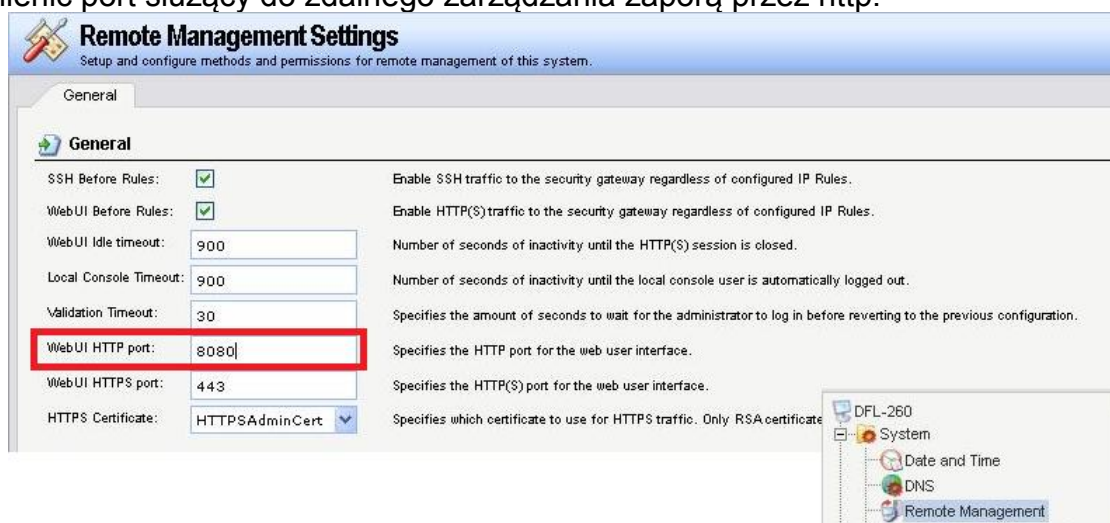
2. Uwierzytelnianie dostępu do Internetu



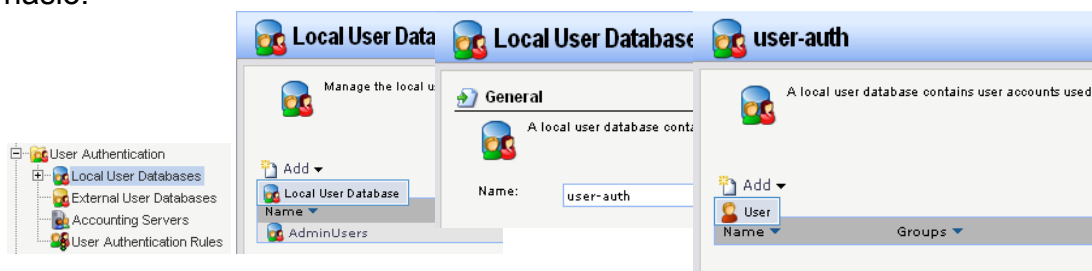
Dopuszczenie użytkownika do Internetu nastąpi po jego uwierzytelnieniu się poprzez podanie nazwy użytkownika i hasła na stronie logowania. Dane do uwierzytelniania mogą zostać pobrane z lokalnej bazy danych lub z serwera typu RADIUS. Wylogowanie może nastąpić ręcznie lub po upływie ustawionego czasu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

The screenshot shows the 'userauth' configuration window. The 'General' tab is selected and highlighted with a red rectangle. The configuration fields are as follows:

Field	Value
Name	userauth
Authentication agent	HTTP
Authentication Source	Local
Interface	lan
Originator IP	lannet
Terminator IP	(None)

On the right side, there is a tree view showing the configuration hierarchy: User Authentication, Local User Databases (AdminUsers, users), External User Databases, Accounting Servers, User Authentication Rules (highlighted), and Authentication Settings.

Below the General tab is a 'Comments' section with a text area.

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

The screenshot shows the 'Timeouts' tab of the 'userauth' configuration window. The configuration fields are as follows:

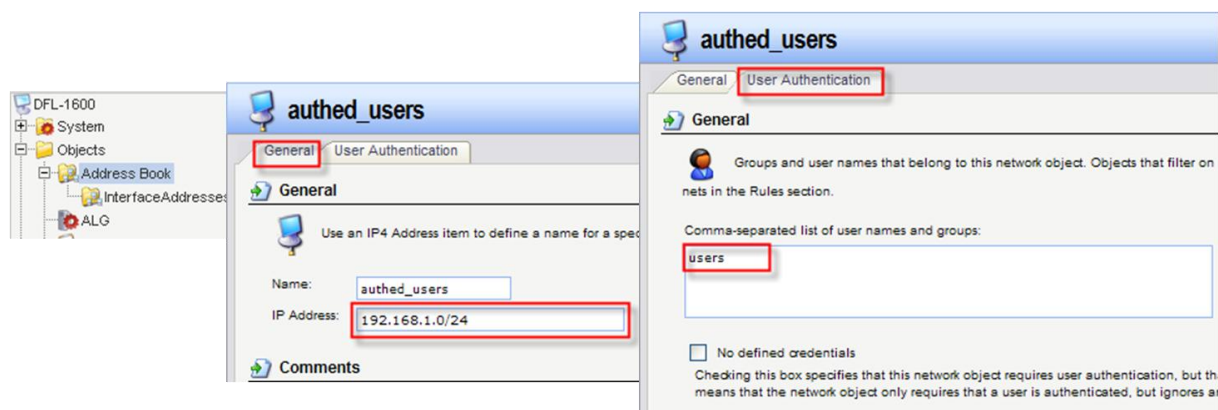
Field	Value	Unit
Idle Timeout	1800	seconds
Session Timeout	3600	seconds

There is a checkbox labeled 'Use timeouts received from the authentication server.' which is unchecked. Below it is a note: 'Note that if no timeouts are received, OR if this checkbox is unchecked, the above settings will be used.'

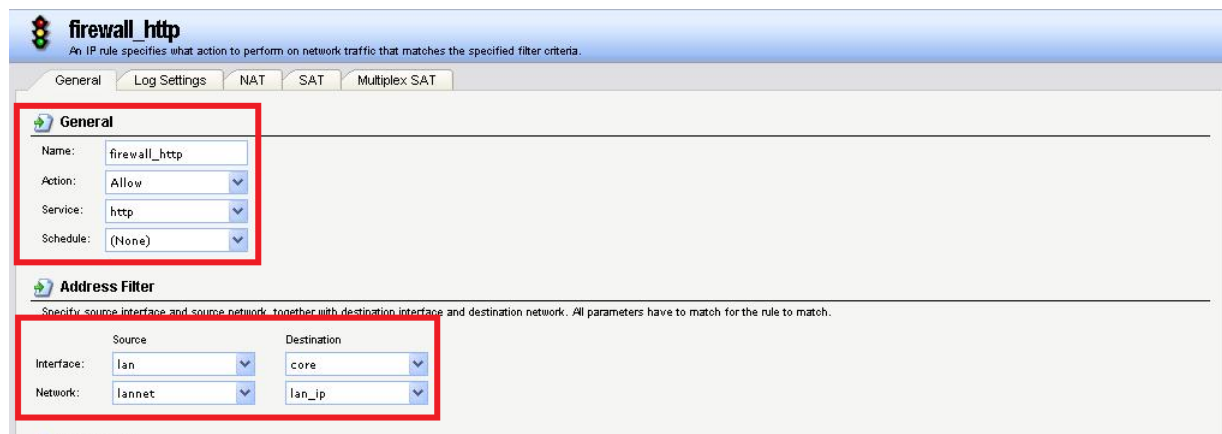
At the bottom, there are two dropdown menus: 'RADIUS Method' set to 'Unencrypted password (PAP)' and 'Local User DB' set to 'users'.

On the right side, there is a tree view showing the configuration hierarchy: User Authentication, Local User Databases (AdminUsers, users), External User Databases, Accounting Servers, User Authentication Rules (highlighted), and Authentication Settings.

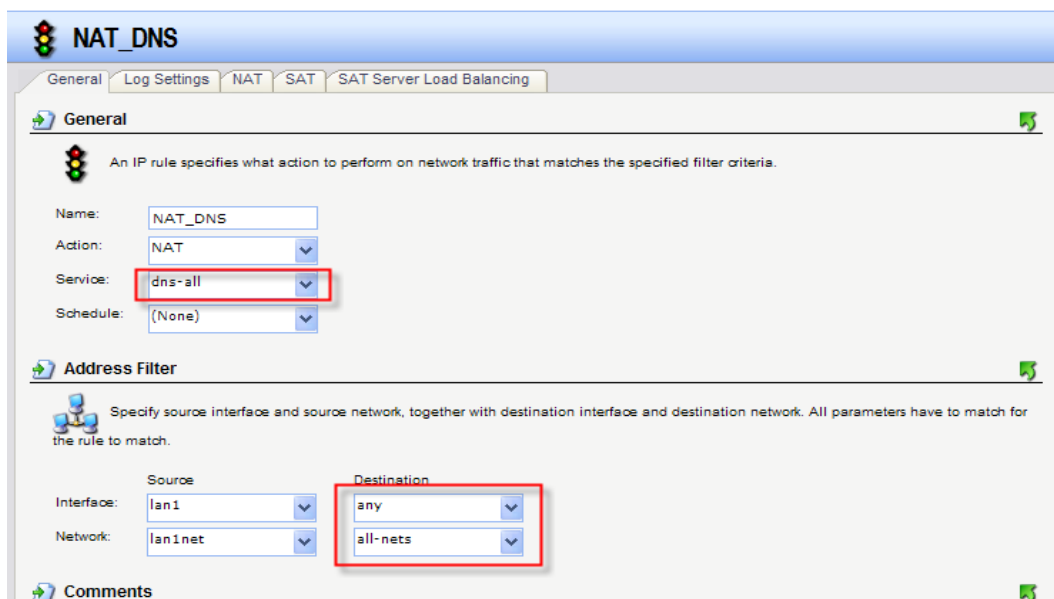
W książce adresowej utworzyć obiekt dla uwierzytelniania użytkowników. Wprowadzić grupę adresów IP oraz nazwę grupy użytkowników.



Usunąć istniejące reguły LAN to WAN. Utworzyć regułę 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) zezwalającą na ruch do serwerów DNS.



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

NAT_all
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: NAT_all
Action: NAT
Service: all_services
Schedule: (None)

Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source		Destination	
Interface:	lan	any	
Network:	auth_users	all-nets	

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

HTTP_FRW
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: HTTP_FRW
Action: SAT
Service: http
Schedule: (None)

Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source		Destination	
Interface:	lan	any	
Network:	lannet	all-nets	

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

http_fwd
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

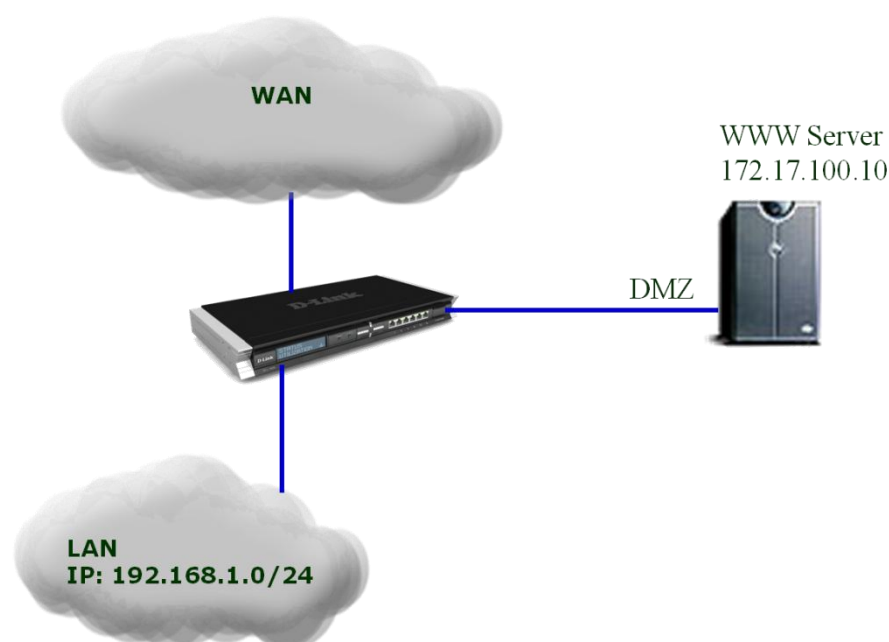
Name: http_fwd
Action: Allow
Service: http
Schedule: (None)

Address Filter
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source		Destination	
Interface:	lan	any	
Network:	lannet	all-nets	

Zapisać i aktywować konfigurację.

3. Mapowanie portu (serwer wirtualny)



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

The screenshot shows the 'SERVER_ADDR' configuration window. It has two tabs: 'General' and 'User Authentication'. The 'General' tab is active, showing fields for 'Name' (SERVER_ADDR) and 'Address' (172.17.100.10). There is also a 'Comments' field with the text 'Adres serwera dołączonego do DMZ'. At the bottom are 'OK' and 'Cancel' buttons.

Utworzyć regułę IP wykonującą akcje SAT.

The screenshot shows the 'HTTP-map' configuration window. It has two tabs: 'General' and 'Log Settings'. The 'General' tab is active, showing fields for 'Name' (HTTP-map), 'Action' (SAT), 'Service' (http-in), and 'Schedule' (None). There is also an 'Address Filter' section with 'Source' and 'Destination' fields. The 'Source' field has 'Interface' set to 'any' and 'Network' set to 'all-nets'. The 'Destination' field has 'Interface' set to 'core' and 'Network' set to 'lan_ip'. At the bottom are 'OK' and 'Cancel' buttons.

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

The screenshot shows the Mikrotik WinBox interface for configuring an IP rule named "HTTP-map-NAT". The "General" tab is active. The "Name" field is "HTTP-map-NAT". The "Action" is set to "NAT". The "Service" is "http-in". The "Schedule" is "(None)". The "Address Filter" section is also visible, with "Interface" set to "lan" and "Network" set to "all-nets". The "Destination" interface is "core" and the "Destination" network is "lan_ip".

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

The screenshot shows the Mikrotik WinBox interface for configuring an IP rule named "allow-HTTP". The "General" tab is active. The "Name" field is "allow-HTTP". The "Action" is set to "Allow". The "Service" is "http-in". The "Schedule" is "(None)". The "Address Filter" section is also visible, with "Interface" set to "any" and "Network" set to "all-nets". The "Destination" interface is "core" and the "Destination" network is "lan_ip".

Zapisać i aktywować konfigurację.