Configuration examples for the D-Link NetDefend Firewall series

DFL-210/800/1600/2500

Last update: 2007-01-17

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

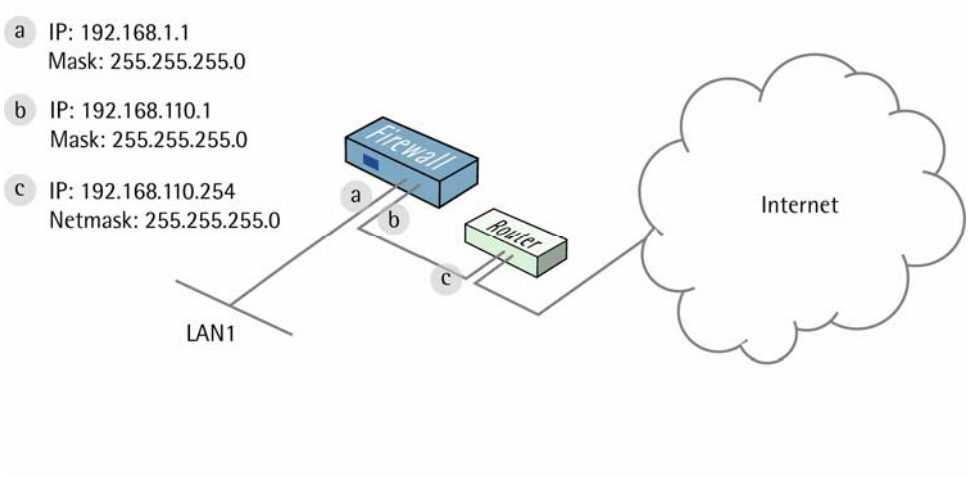
Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

The screenshots in this document is from firmware version 2.11.02. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

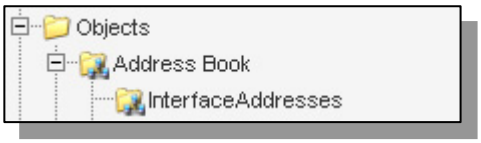
Require user authentication for web access

This scenario shows how to configure the firewall to require user authentication before local users can browse the Internet. The user will automatically be redirected to the login page if not already authenticated. In the end of this guide there is also an explanation of an alternative set up - how to configure the firewall to use authentication without the automatic redirection.



1. **Addresses**

Go to *Objects -> Address book -> InterfaceAddresses*:



Edit the following items:
Change **lan_ip** to **192.168.1.1**
Change **lannet** to **192.168.1.0/24**
Change **wan1_ip** to **192.168.110.1**
Change **wan1net** to **192.168.110.0/24**

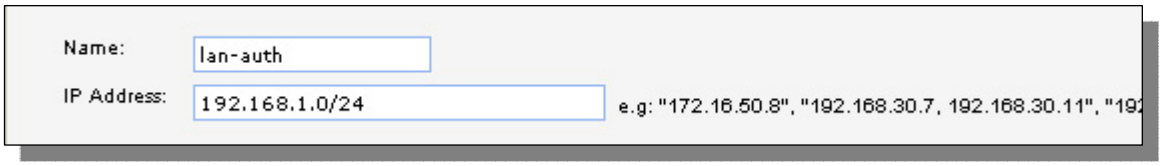
Add a new **IP address** object:
Name: **gw-world**
IP Address: **192.168.110.254**

Click **OK**.

Add a new **IP address** object.

In the **General** tab:

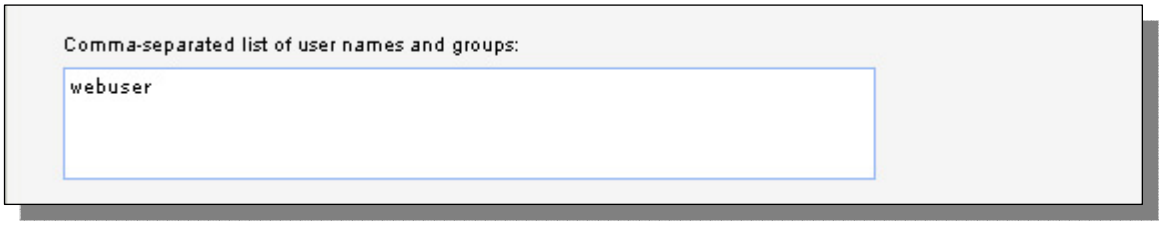
General:



Name: **lan-auth**
IP Address: **192.168.1.0/24**

In the **User Authentication** tab:

General:



Enter **webuser** in the textbox.

Click **Ok**.

2. Interfaces

Go to *Interfaces -> Ethernet*.

Edit the **wan1** interface.

In the **General** tab:

General:

Name: **wan1**
IP Address: **wan1_ip**
Network: **wan1net**
Default Gateway: **gw-world**

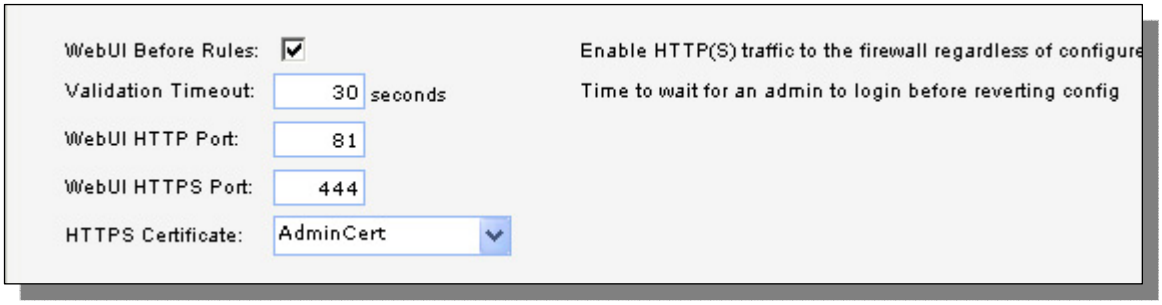
Click **Ok**.

3. Remote Management

The port used for the web user interface has to be changed, since web user authentication will use port 80.

Go to *System -> Remote Management*.

Click **Modify advanced settings**.



General:

WebUI HTTP Port: **81**
WebUI HTTPS Port: **444**

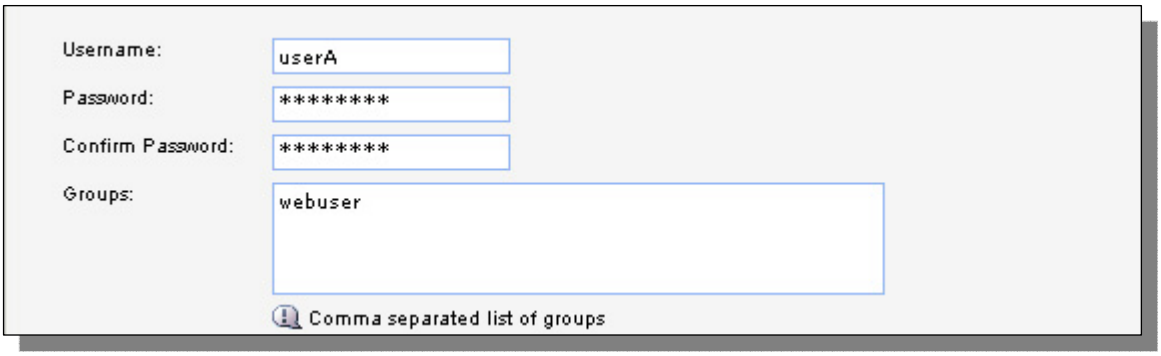
Click **Ok**.

4. User database

Go to *User Authentication -> Local User Databases*.

Add a new **Local User Database** called **`WebUsers`**.

In the new folder, add a new **User**.



General:

Username: **`userA`**
Enter a **Password** and confirm it.
Group: **`webuser`**

Click **Ok**.

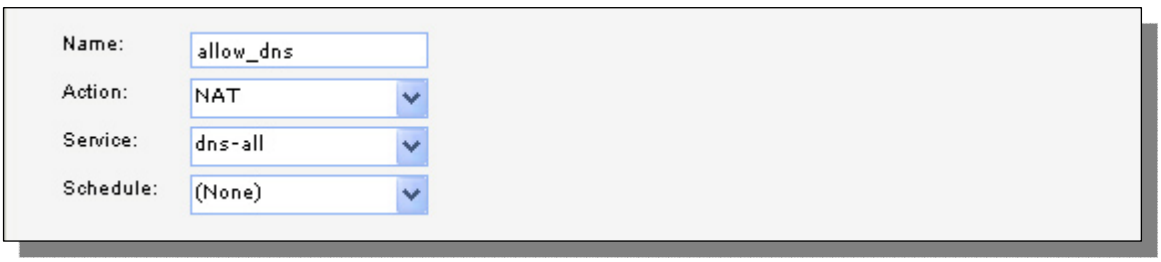
5. Rules

Go to *Rules -> IP Rules -> lan_to_wan1*.

Add a new **IP Rule**.

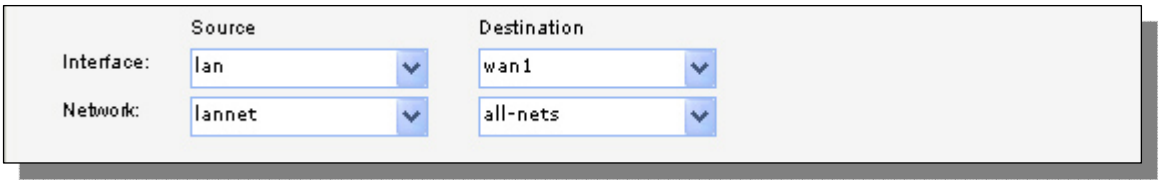
In the **General** tab:

General:



Name: **`allow_dns`**
Action: **`NAT`**
Service: **`dns-all`**
Schedule: **`(None)`**

Address Filter:



Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **wan1**
Destination Network: **all-nets**

Click **Ok**.

The rule just added will allow access from lan to the DNS servers.

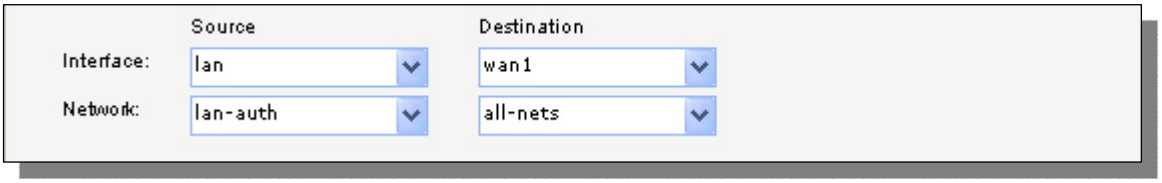
Edit the **allow_ftp-passthrough** **IP Rule**.

In the **General** tab:

General:

Name: **allow_passthrough**
Action: **NAT**
Service: **ftp-passthrough**
Schedule: **(None)**

Address Filter:



Source Interface: **lan**
Source Network: **lan-auth**
Destination Interface: **wan1**
Destination Network: **all-nets**

Click **Ok**.

We modified the ftp-passthrough rule to only allow authenticated users to connect to the Internet using FTP (by changing source network to lan-auth).

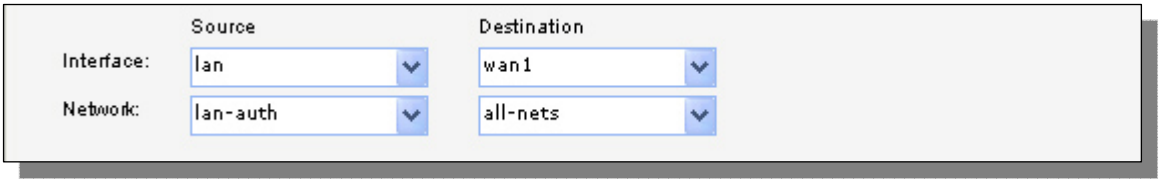
Edit the **allow_standard** IP Rule.

In the General tab:

General:

Name: **allow_standard**
Action: **NAT**
Service: **all_tcpudp**
Schedule: **(None)**

Address Filter:



Source Interface: **lan**
Source Network: **lan-auth**
Destination Interface: **wan1**
Destination Network: **all-nets**

The modified allow_standard rule will only allow authenticated users to connect to the Internet.

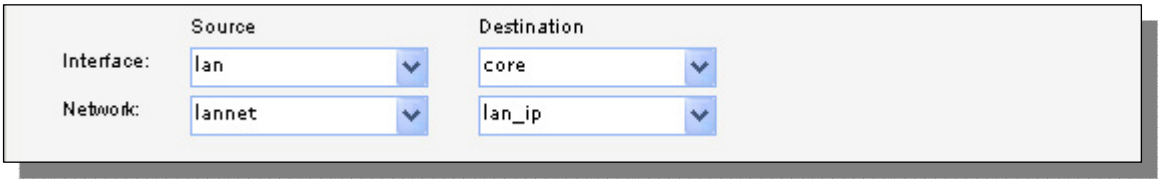
Add a new IP Rule.

In the General tab:

General:

Name: **allow_httpauth**
Action: **Allow**
Service: **http-all**
Schedule: **(None)**

Address Filter:



Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **core**
Destination Network: **lan_ip**

Click **Ok**.

This rule will allow users to go directly to the login page, eg by entering the lan IP address in the browser (**http://192.168.1.1**).

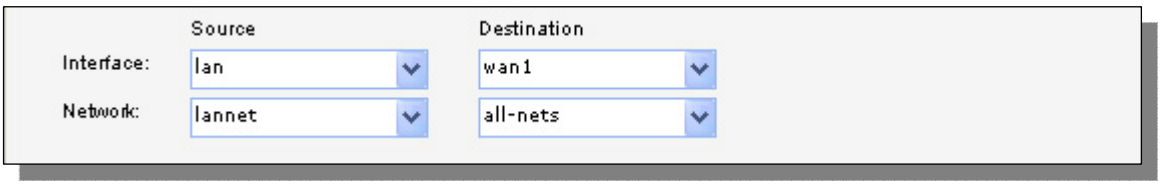
Add a new **IP Rule**.

In the **General** tab:

General:

Name: **allow_httpauth**
Action: **SAT**
Service: **http-all**
Schedule: **(None)**

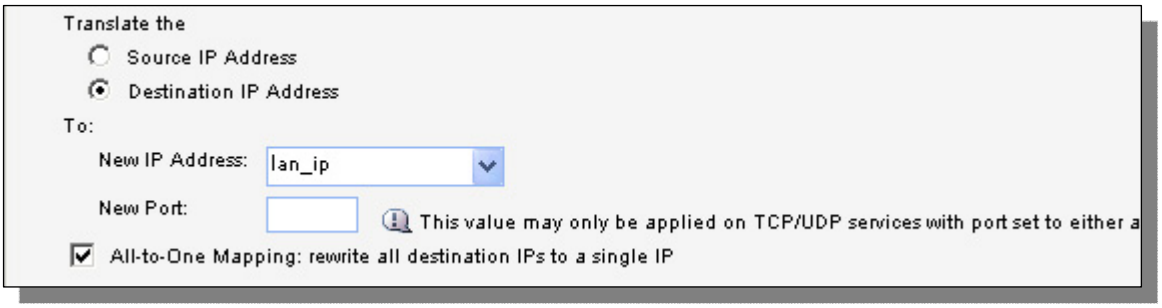
Address Filter:



Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **wan1**
Destination Network: **all-nets**

In the **SAT** tab:

General:



Select **Destination IP Address**
Select To **New IP Address**: **lan_ip**
Enable **All-to-One Mapping**.

Click **Ok**.

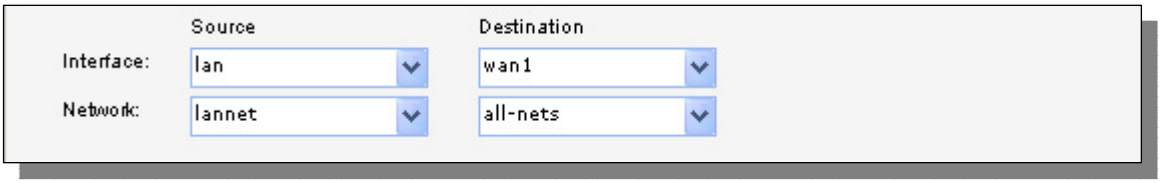
Add a new **IP Rule**.

In the **General** tab:

General:

Name: **allow_httpauth**
Action: **Allow**
Service: **http-all**
Schedule: **(None)**

Address Filter:



Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **wan1**
Destination Network: **all-nets**

Click **Ok**.

The last to rules will redirect all unauthenticated HTTP users to the login page.

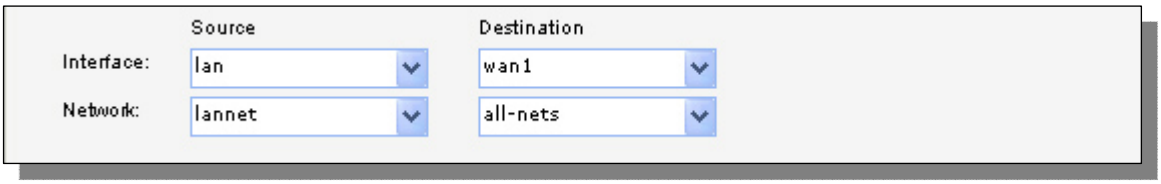
Add a new **IP Rule**.

In the **General** tab:

General:

Name: **`reject_all`**
Action: **`Reject`**
Service: **`all_services`**
Schedule: **`(None)`**

Address Filter:



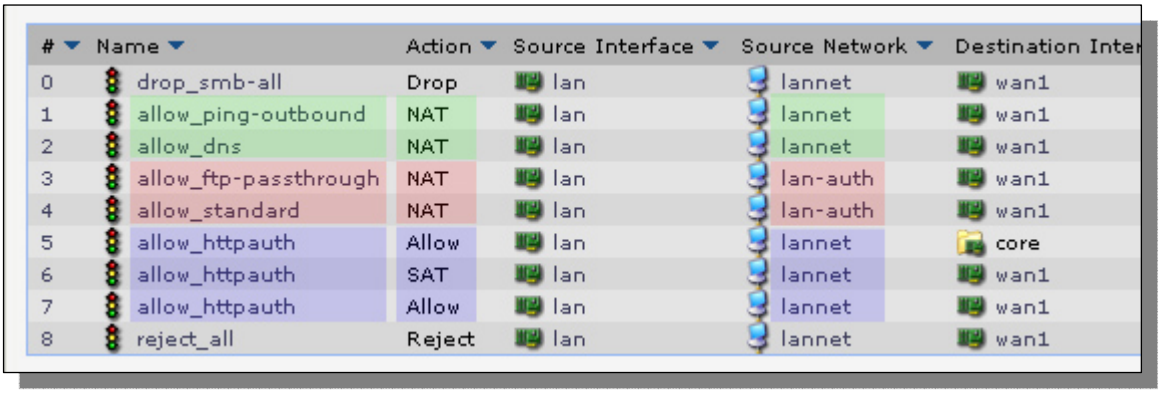
Source Interface: **`lan`**
Source Network: **`lannet`**
Destination Interface: **`wan1`**
Destination Network: **`all-nets`**

Click **Ok**.

The last rule will reject all traffic from unauthenticated users instead of just dropping it.

Change the order of the rules so that the newly created allow_dns comes before the ftp rule. The order of the rules is important. If they are in wrong order, it will not work as expected.

Your list should now look like this (if you started from a factory default configuration):



#	Name	Action	Source Interface	Source Network	Destination Inter
0	drop_smb-all	Drop	lan	lannet	wan1
1	allow_ping-outbound	NAT	lan	lannet	wan1
2	allow_dns	NAT	lan	lannet	wan1
3	allow_ftp-passthrough	NAT	lan	lan-auth	wan1
4	allow_standard	NAT	lan	lan-auth	wan1
5	allow_httpauth	Allow	lan	lannet	core
6	allow_httpauth	SAT	lan	lannet	wan1
7	allow_httpauth	Allow	lan	lannet	wan1
8	reject_all	Reject	lan	lannet	wan1

First we have two rules highlighted with green color. These two will allow ping and DNS for all users. Then we have two rules marked with red, that only will allow authenticated users to use the FTP service (using the FTP ALG) and all other UDP and TCP based services. Finally there are three rules marked with blue. The first one will allow users to connect directly to the firewall for authentication. The other two will redirect unauthenticated HTTP users to the firewall for authentication.

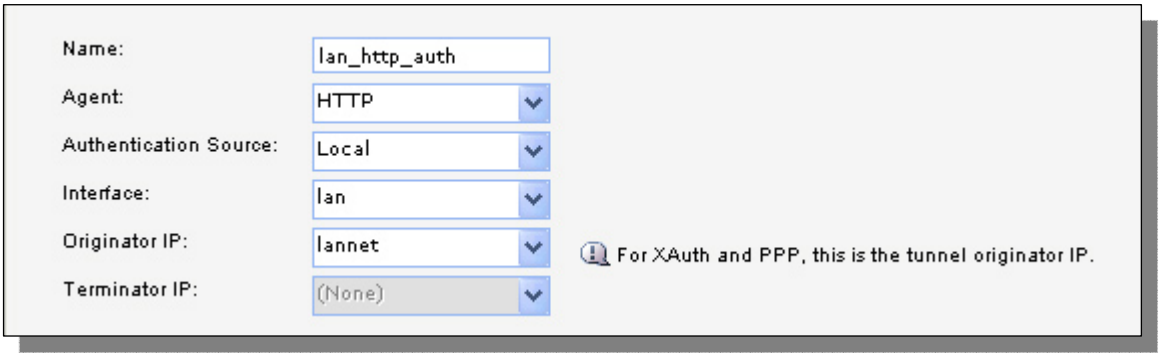
6. User authentication

Go to *User Authentication -> User Authentication Rules*.

Add a new **User Authentication Rule**.

In the **General** tab:

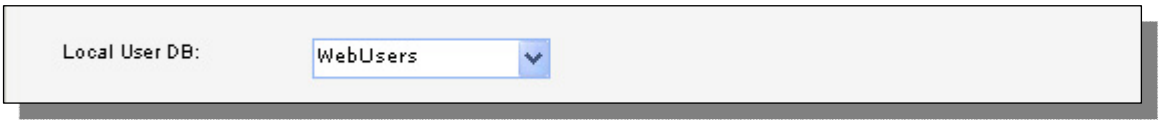
General:



Name: **`lan_http_auth`**
Agent: **`HTTP`**
Authentication Source: **`Local`**
Interface: **`lan`**
Originator IP: **`lannet`**

In the **Authentication Options** tab:

General:



Local User DB: **`WebUsers`**

In the **HTTP(S) Agent Options** tab:

General:

Login Type: **`HTMLForm`**

In the **Restrictions** tab:

Timeouts:

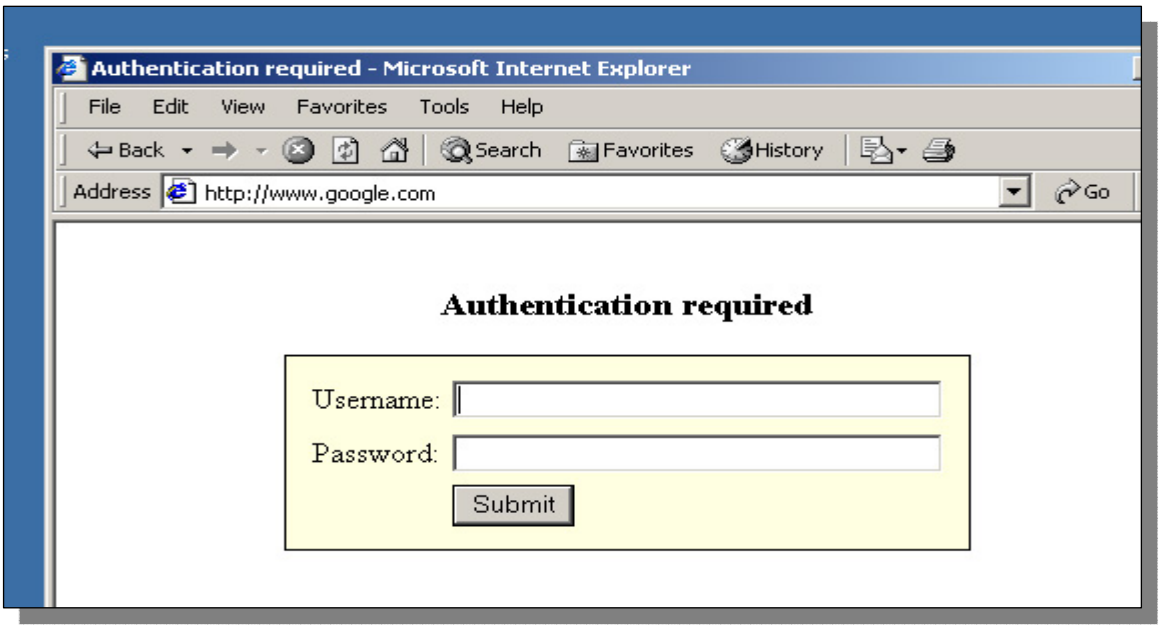
Idle Timeout: **`600`** seconds

Click **Ok**.

Users that are idle for more then 10 minutes (600 seconds) will automatically be logged out.

Save and activate the configuration.

When a user from the lan network tries to browse the Internet with his/her browser, he/she will be redirected to the log in page and must log in.



Enhancements:
More users can be added to the **`WebUsers`** database. Just make sure the new users also belong to the **`webuser`** group (the group textbox in step 4).

Note!
The port of the firewall web user interface has been changed. When you connect to the firewall from now on you will have to specify port 81. If the address earlier was **`http://192.168.1.1`** you will now have to use **`http://192.168.1.1:81`**. If https is used, the address will be **`https://192.168.1.1:444`**.

Note!
Some browsers may cache webpages. Since we redirected the browsers first attempt to access a website on the Internet, the browser may cache the login page for that URL. Eg, if the user enters www.google.com, logs in and tries to connect to www.google.com again the browser might display the login page again. A reload/refresh page in the browser should solve the problem.

Note!
If there is a proxy installed in the network, some additional modifications have to be done. If the proxy uses port 8080, add this port to the http-all service (under *Objects -> Services*). The destination ports should be **`80,443,8080`**.

Alternative setups:
In this example we automatically redirected the user to the login page when not authenticated. A simpler example would be to remove the last two **`allow_httpauth`** rules (SAT and Allow, leave the first Allow).

The user then will have to manually connect to the firewall (**`http://192.168.1.1`**) first to log in.

It is also possible to change the setup to only require authentication for certain services, like HTTP. All other services would be accessible for all users.