Configuration examples for the D-Link NetDefend Firewall series DFL-260/860

Scenario: How to configure User Authentication for multiple groups

Last update: 2008-04-29

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-860. 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 2.20.03. 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.

This scenario demonstrates how the firewall can control user name access to curtain services.

Example;

A School needs three user groups containing Students, Teachers and staff.

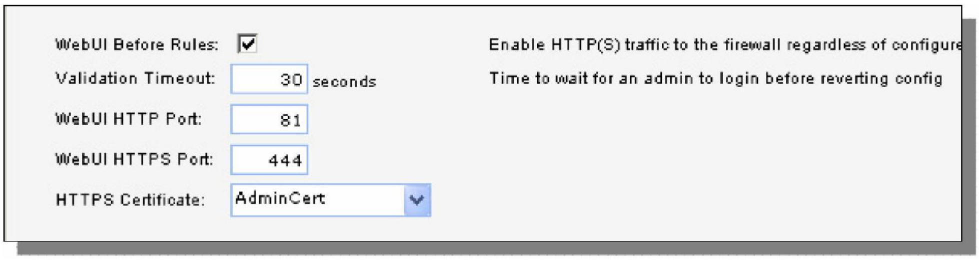
The requirements are that every user can login to the same PC, but each group has different access rights.

E.G. Teachers can access youtube, students can not access youtube

Step 1: 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.

Click **Modify advanced settings.**



WebUI Before Rules: ☑ Enable HTTP(S) traffic to the firewall regardless of configure

Validation Timeout: 30 seconds Time to wait for an admin to login before reverting config

WebUI HTTP Port: 81

WebUI HTTPS Port: 444

HTTPS Certificate: AdminCert

General:

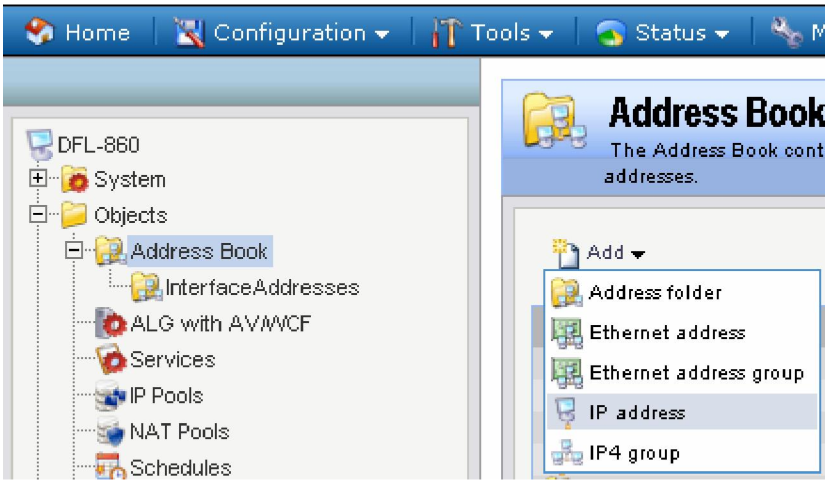
WebUI HTTP Port: 81
WebUI HTTPS Port: 444

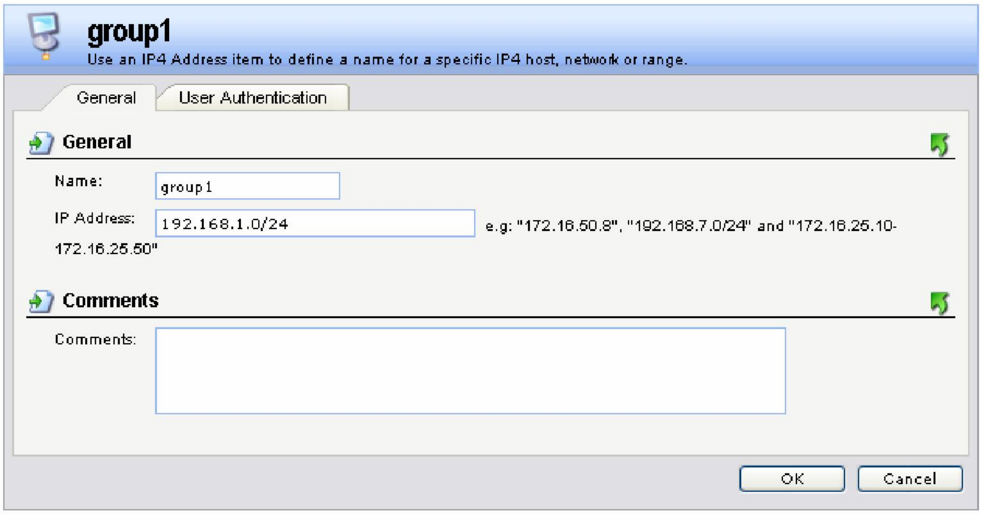
Click Ok.

Step 2: Addresses

Go to Objects -> Address book -> InterfaceAddresses

Add a new **IP address** object:




group1
Use an IP4 Address item to define a name for a specific IP4 host, network or range.
General
User Authentication
General
Comments
OK
Cancel

Name: group1

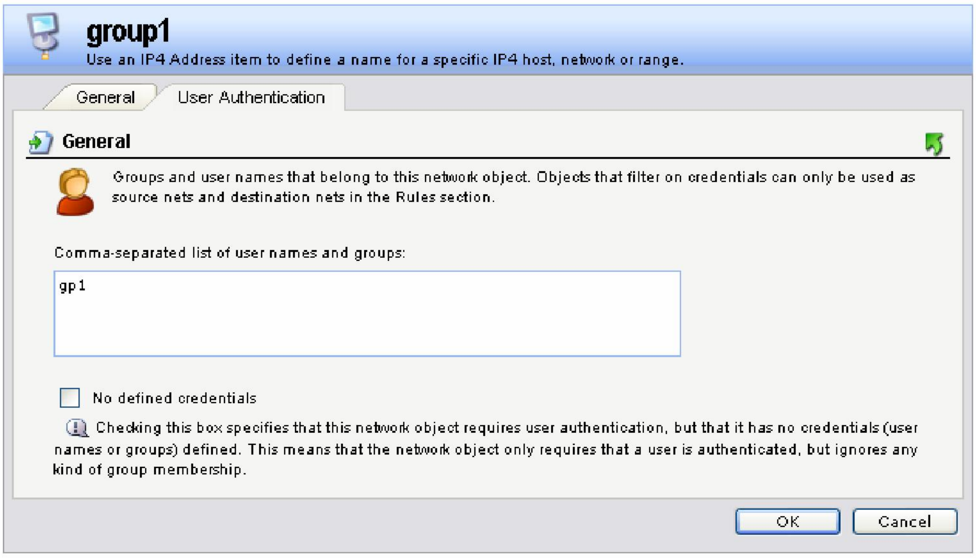
IP Address: 192.168.1.0/24

e.g: "172.16.50.8", "192.168.7.0/24" and "172.16.25.10-172.16.25.50"

Comments:

Name: **group1**
IP Address: **192.168.1.0/24**

Click on **User Authentication** Tab and enter in **gp1** to the white box



group1

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

Groups and user names that belong to this network object. Objects that filter on credentials can only be used as source nets and destination nets in the Rules section.

Comma-separated list of user names and groups:

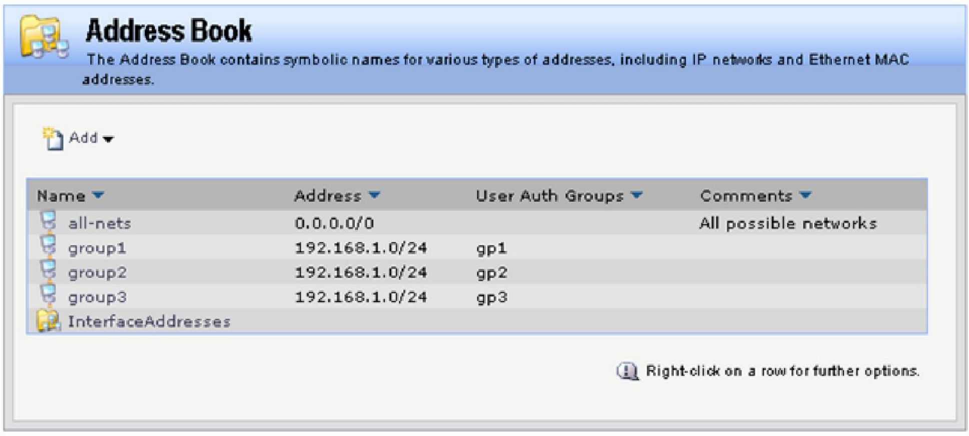
gp1

□ No defined credentials

Checking this box specifies that this network object requires user authentication, but that it has no credentials (user names or groups) defined. This means that the network object only requires that a user is authenticated, but ignores any kind of group membership.

Click **Ok**.

Do the same **three times or how ever many groups you need**.
The IP you enter will be the same for each IP Address



Address Book

The Address Book contains symbolic names for various types of addresses, including IP networks and Ethernet MAC addresses.

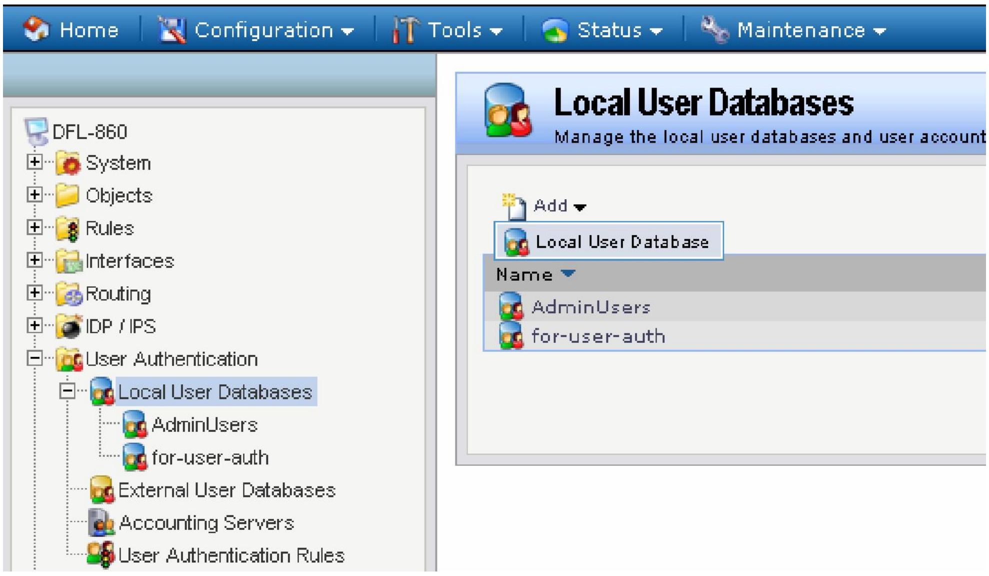
Name	Address	User Auth Groups	Comments
all-nets	0.0.0.0/0		All possible networks
group1	192.168.1.0/24	gp1	
group2	192.168.1.0/24	gp2	
group3	192.168.1.0/24	gp3	
InterfaceAddresses			

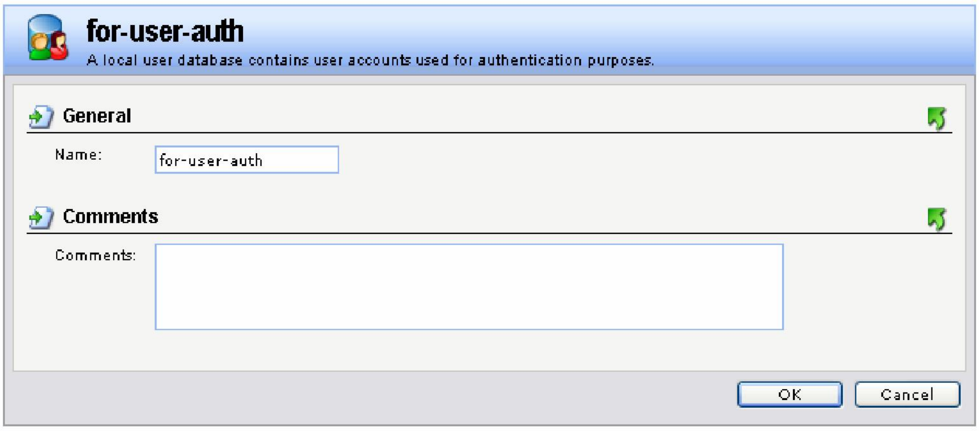
Right-click on a row for further options.

Step 3: User Databases

Go to User Authentication -> Local User Databases.

Add a new **Local User Database**




for-user-auth

A local user database contains user accounts used for authentication purposes.

General

Name: for-user-auth

Comments

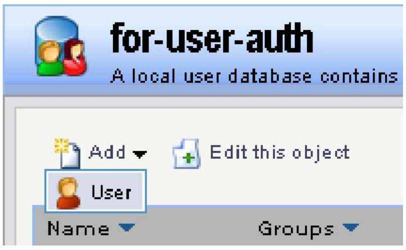
Comments:

General:

Name: **for-user-auth**.

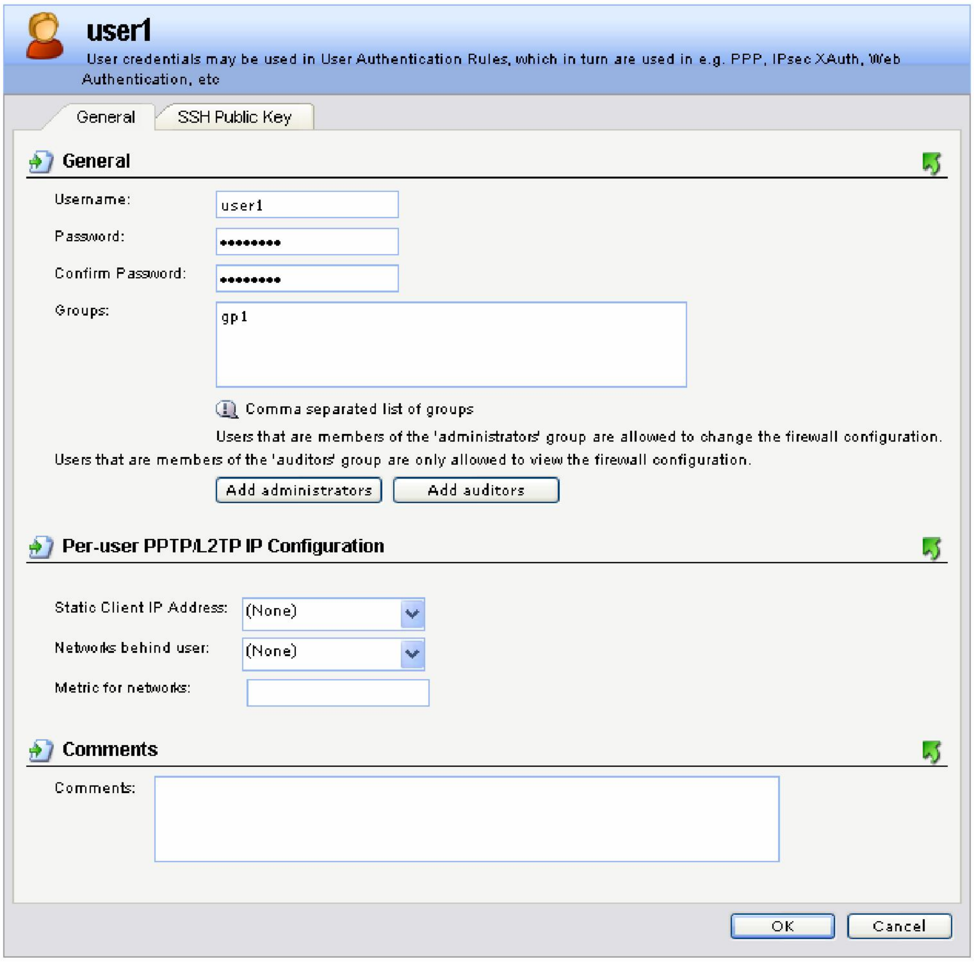
Click **Ok**.

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



for-user-auth

A local user database contains



user1

User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

General

Username: user1

Password: ••••••••

Confirm Password: ••••••••

Groups: gp1

Comma separated list of groups

Users that are members of the 'administrators' group are allowed to change the firewall configuration.

Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

Per-user PPTP/L2TP IP Configuration

Static Client IP Address: (None)

Networks behind user: (None)

Metric for networks:

Comments

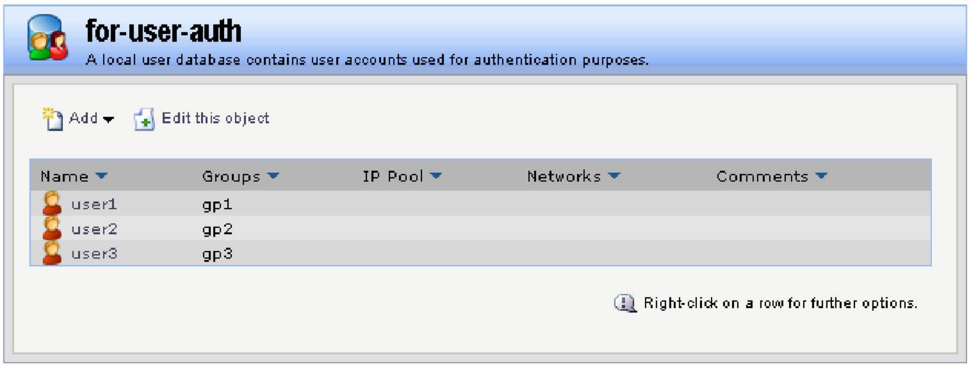
Comments:

General:

Username: user1
Password: Enter a Password and confirm it.
Group: gp1

Click Ok.

Keep adding each user into the database and the group that they will be a member of.



for-user-auth

A local user database contains user accounts used for authentication purposes.

Name	Groups	IP Pool	Networks	Comments
user1	gp1			
user2	gp2			
user3	gp3			

Right-click on a row for further options.

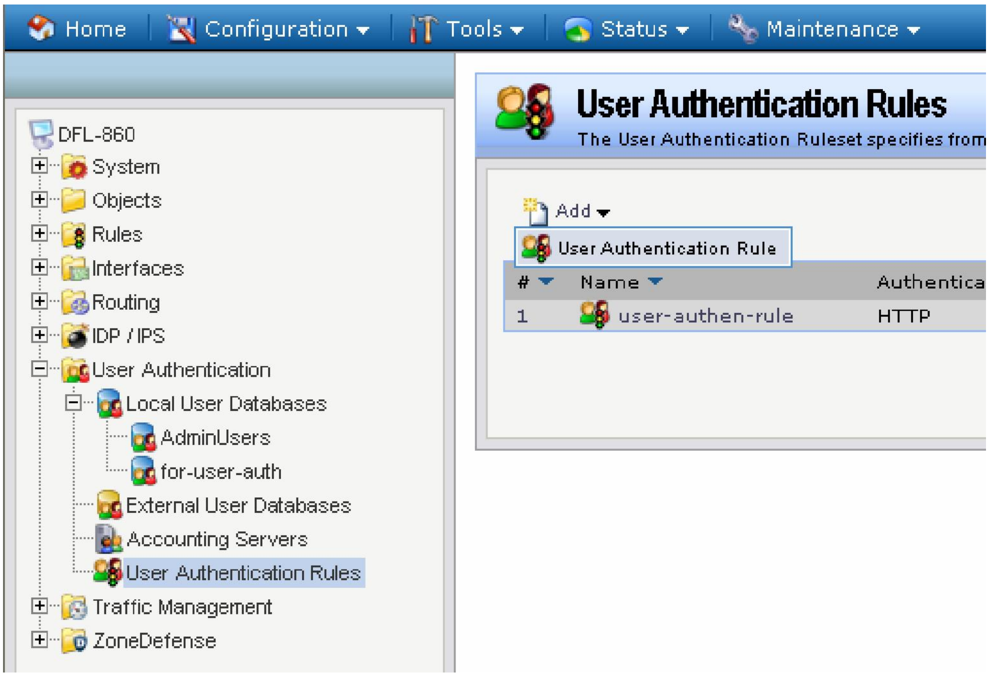
If you have five users that you want in the same group add the five users, each one will have a different username but the group name will be the same.

Or if you want you can have one username and this username can be used by several people (See in User rules how to allow the same login name several time).

Step 4: User Rules

Go to User Authentication -> User Authentication Rules.

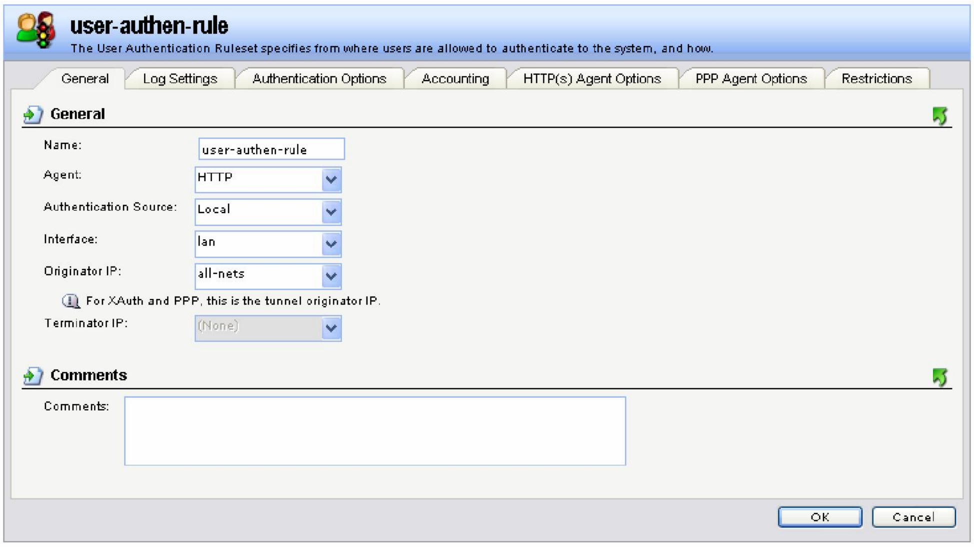
Add a new **User Authentication Rule**



User Authentication Rules

The User Authentication Ruleset specifies from

#	Name	Authentica
1	user-authen-rule	HTTP



user-authen-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General

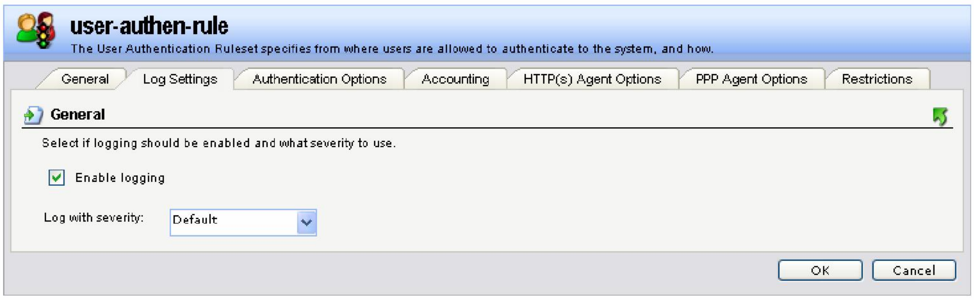
Name: user-authen-rule
Agent: HTTP
Authentication Source: Local
Interface: lan
Originator IP: all-nets
For XAuth and PPP, this is the tunnel originator IP.
Terminator IP: (None)

Comments

Comments:

General:

Name: **user-authen-rule**
Agent: **HTTP**
Authentication Source: **Local**
Interface: **Lan**
Originator IP: **all-nets**



user-authen-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General

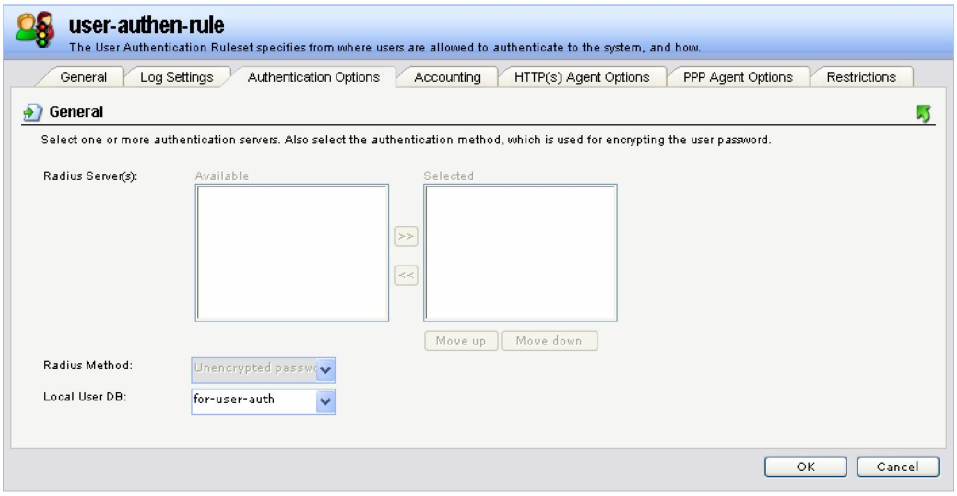
Select if logging should be enabled and what severity to use.

☑ Enable logging

Log with severity: Default

Log Setting:

Enable Logging



user-authen-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General

Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

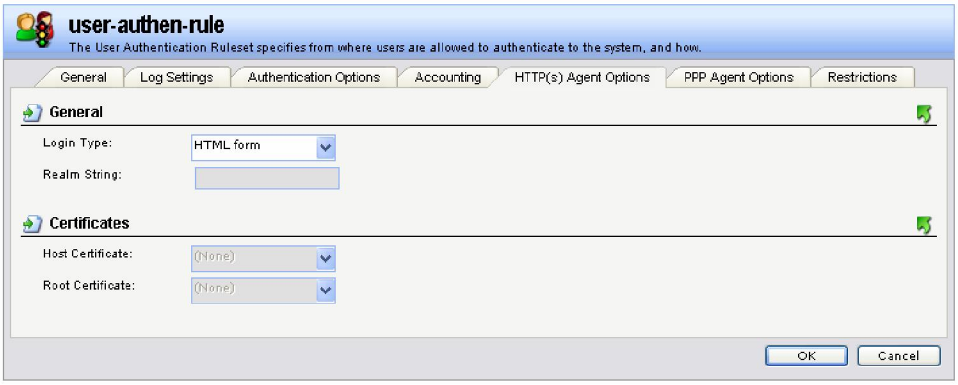
Radius Server(s):

Radius Method: Unencrypted passw

Local User DB: for-user-auth

Authentication Options:

Under the Local User DB select **for-user-auth**



user-authen-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General

Login Type: HTML form

Realm String:

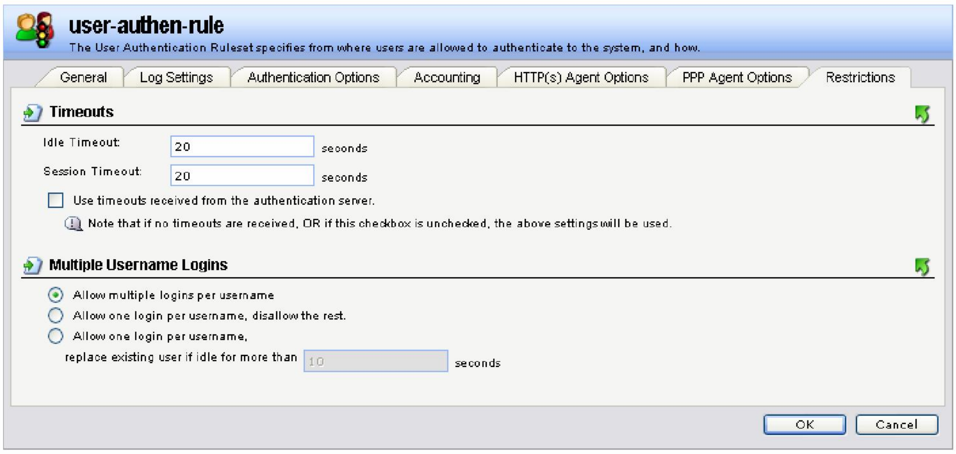
Certificates

Host Certificate: (None)

Root Certificate: (None)

HTTP(s) Agent Options:

Login Type: HTML form



user-authen-rule

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

Timeouts

Idle Timeout: 20 seconds

Session Timeout: 20 seconds

□ Use timeouts received from the authentication server.

Note that if no timeouts are received, OR if this checkbox is unchecked, the above settings will be used.

Multiple Username Logins

● Allow multiple logins per username

○ Allow one login per username, disallow the rest.

○ Allow one login per username,
replace existing user if idle for more than 10 seconds

Restrictions:

Idle and Session timeout can be left as default or changed to affect the user once they have logged in

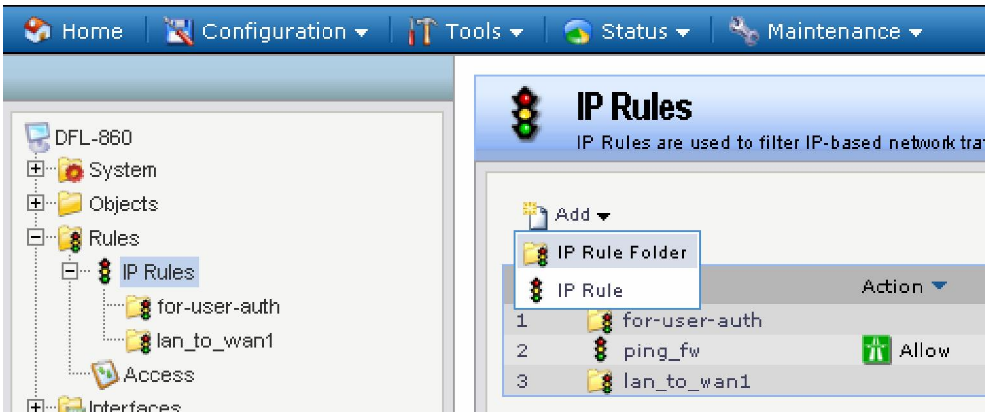
Multiple Username Logins can be change to allow the same username from several PCs.

Click **Ok**.

Step 5: Rules

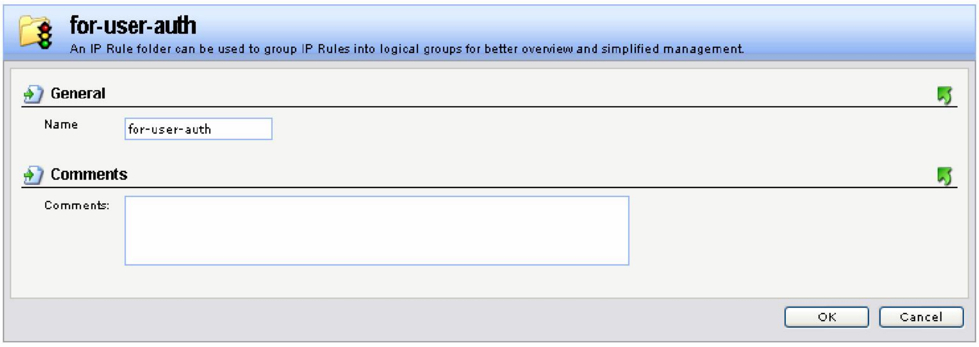
Go to Rules > IP Rules

Add **IP Rule Folder**



1	for-user-auth	
2	ping_fw	Allow
3	lan_to_wan1	

Name it **for-user-auth**



for-user-auth

An IP Rule folder can be used to group IP Rules into logical groups for better overview and simplified management.

General

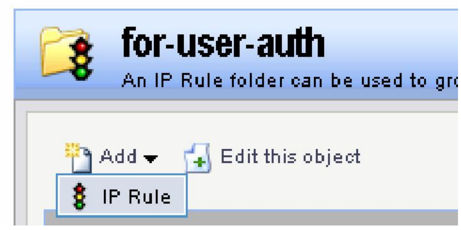
Name: for-user-auth

Comments

Comments:

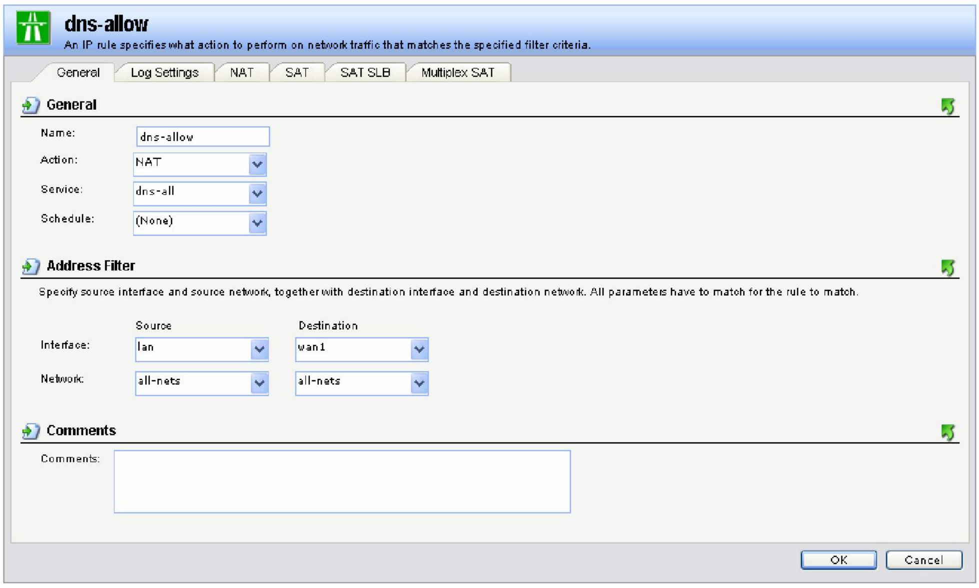
Click on **for-user-auth** to access this folder

Add **IP Rule** (Total of 6 rules needed)



for-user-auth

An IP Rule folder can be used to gro



dns-allow

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

General

Name: dns-allow

Action: NAT

Service: dns-all

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	wan1
Network:	all-nets	all-nets

Comments

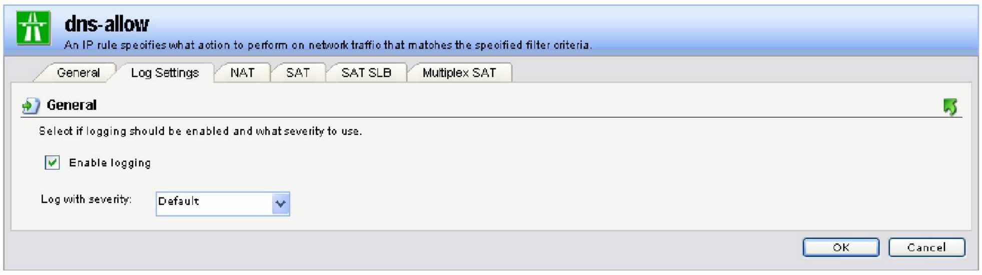
Comments:

General:

Name: **dns-allow**
Action: **NAT**
Service: **dns-all**

Source Interface: **lan**
Source Network: **lannet**

Destination Interface: **wan1**
Destination Network: **all-nets**



dns-allow

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

General

Select if logging should be enabled and what severity to use.

☑ Enable logging

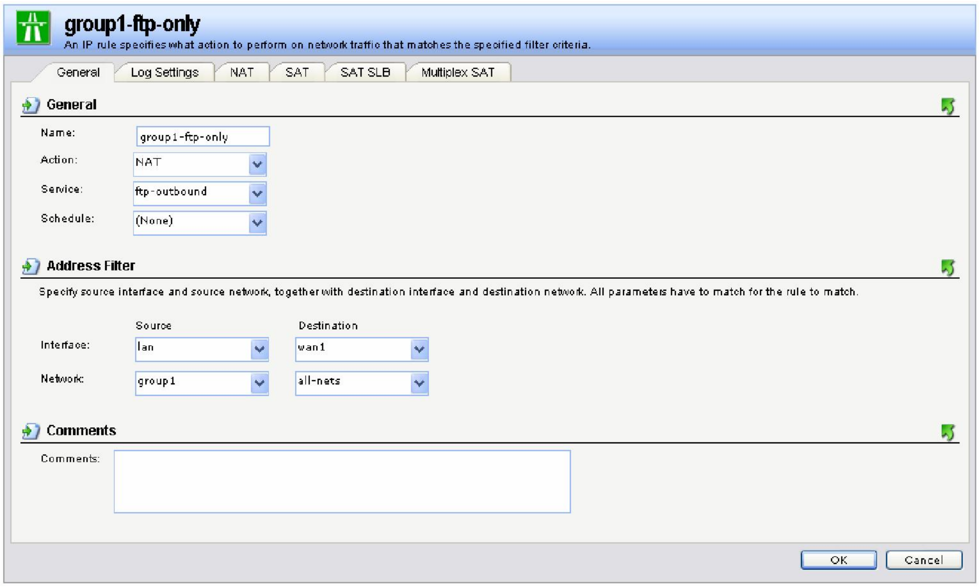
Log with severity: Default

Log Setting:

Enable Logging

Click **Ok**.

Add another rule



group1-ftp-only

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

General

Name: group1-ftp-only
Action: NAT
Service: ftp-outbound
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	wan1
Network:	group1	all-nets

Comments

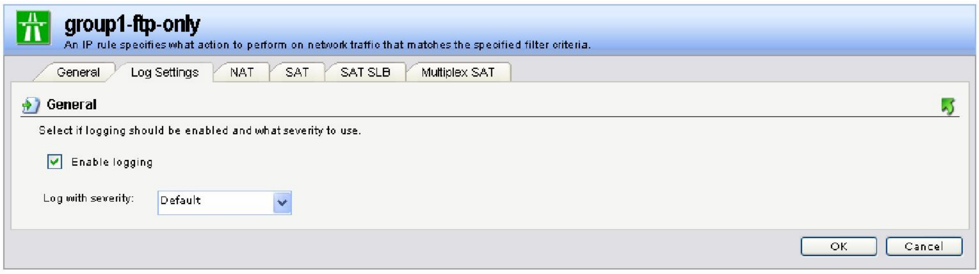
Comments:

General:

Name: **group1-ftp-only** (this will allow ftp access only for group1)
Action: **NAT**
Service: **ftp-outbound**

Source Interface: **lan**
Source Network: **group1**

Destination Interface: **wan1**
Destination Network: **all-nets**



group1-ftp-only

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

General

Select if logging should be enabled and what severity to use.

☑ Enable logging

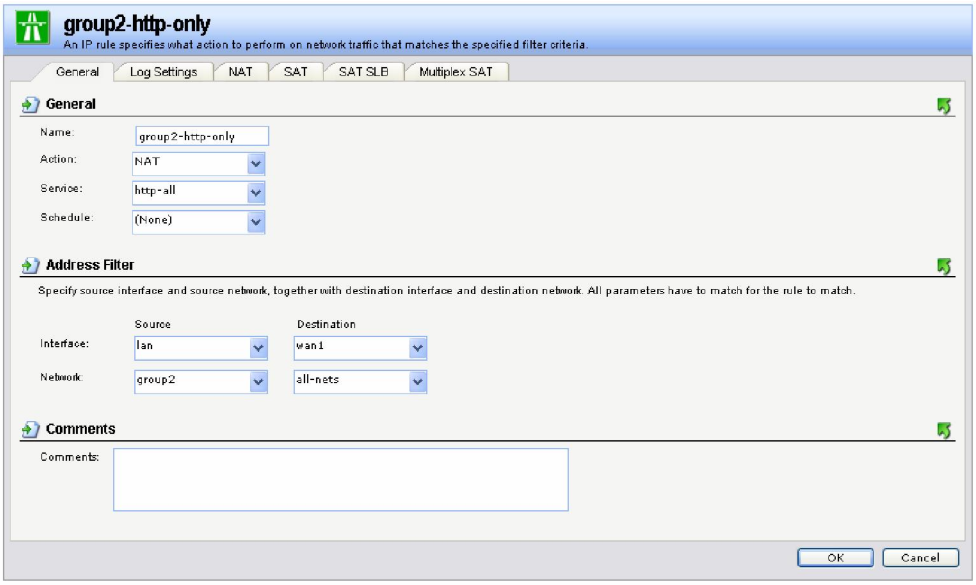
Log with severity: Default

Log Setting:

Enable Logging

Click **Ok**.

Add another rule



group2-http-only

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

General

Name: group2-http-only
Action: NAT
Service: http-all
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	wan1
Network:	group2	all-nets

Comments

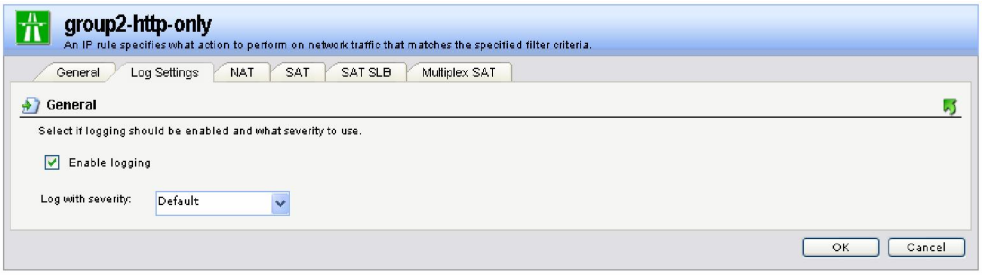
Comments:

General:

Name: **group2-http-only** (this will allow http access only for group2)
Action: **NAT**
Service: **http-all**

Source Interface: **lan**
Source Network: **group2**

Destination Interface: **wan1**
Destination Network: **all-nets**



group2-http-only

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

General

Select if logging should be enabled and what severity to use.

☑ Enable logging

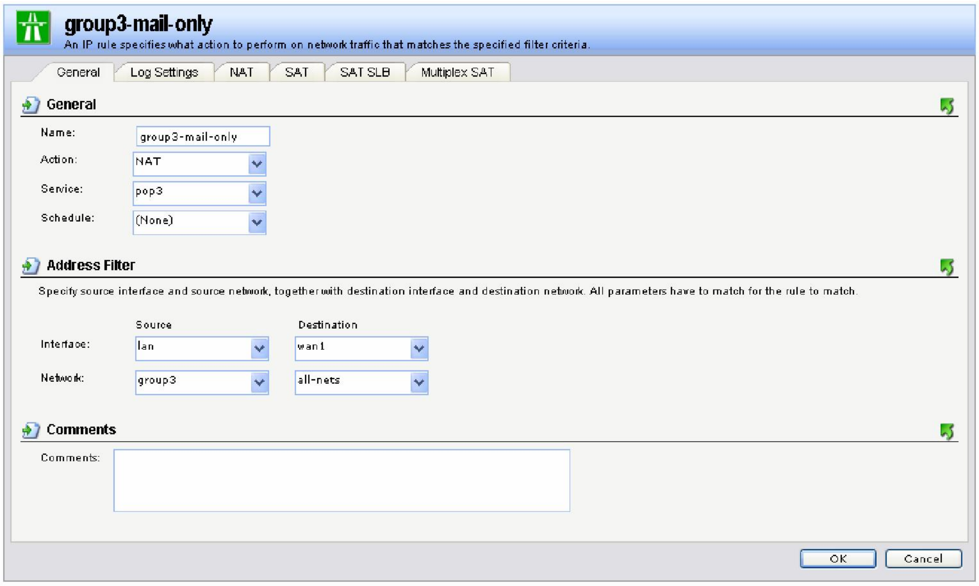
Log with severity: Default

Log Setting:

Enable Logging

Click **Ok**.

Add another rule



group3-mail-only

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

General

Name: group3-mail-only

Action: NAT

Service: pop3

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	wan1
Network:	group3	all-nets

Comments

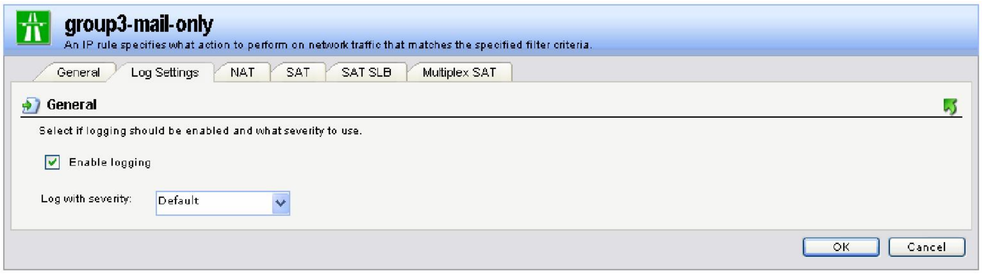
Comments:

General:

Name: **group3-mail-only** (this will allow email access only for group3)
Action: **NAT**
Service: **pop3**

Source Interface: **lan**
Source Network: **group3**

Destination Interface: **wan1**
Destination Network: **all-nets**



group3-mail-only

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

General

Select if logging should be enabled and what severity to use.

☑ Enable logging

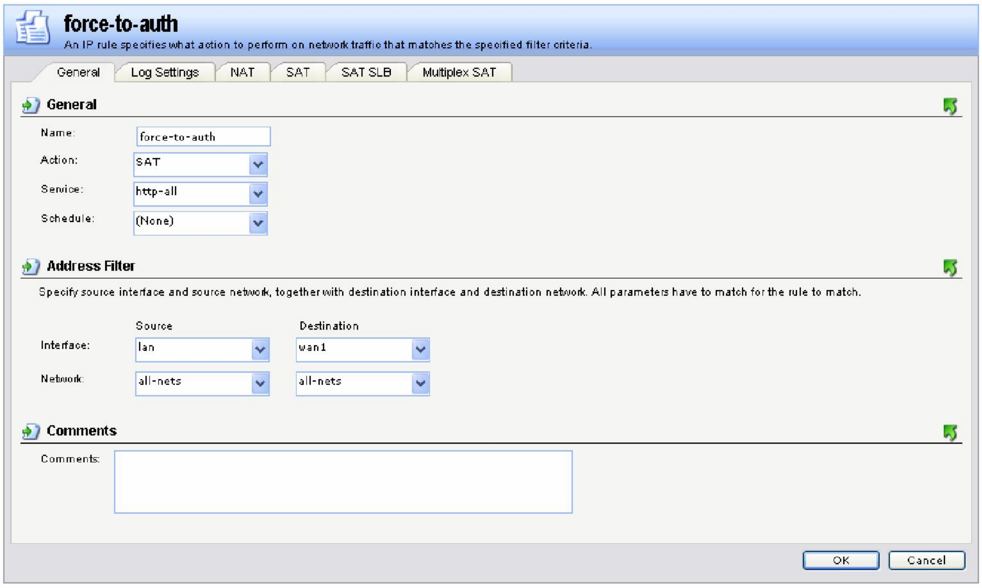
Log with severity: Default

Log Setting:

Enable Logging

Click **Ok**.

Add another rule



force-to-auth

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

General

Name: force-to-auth
Action: SAT
Service: http-all
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	wan1
Network:	all-nets	all-nets

Comments

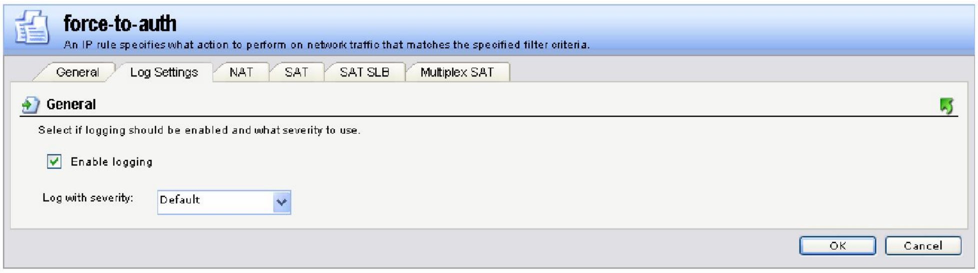
Comments:

General:

Name: **force-to-auth**
Action: **SAT**
Service: **http-all**

Source Interface: **lan**
Source Network: **all-nets**

Destination Interface: **wan1**
Destination Network: **all-nets**



force-to-auth

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

General

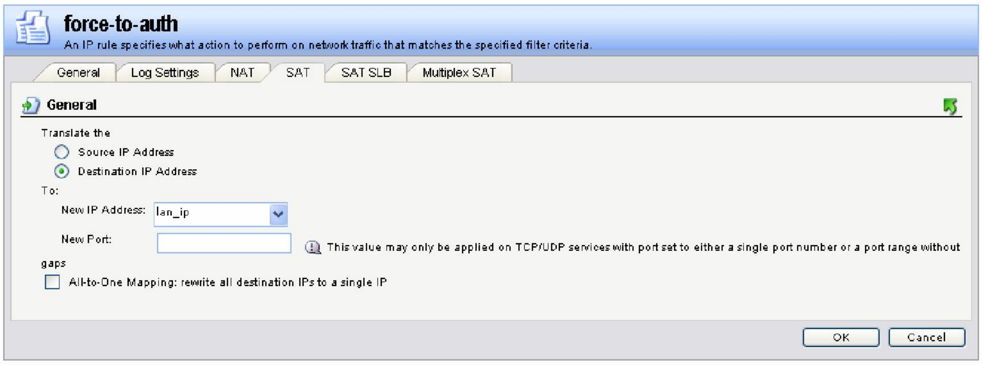
Select if logging should be enabled and what severity to use.

☑ Enable logging

Log with severity: Default

Log Setting:

Enable Logging



force-to-auth

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

General

Translate the

○ Source IP Address

● Destination IP Address

To:

New IP Address: lan_ip

New Port:

This value may only be applied on TCP/UDP services with port set to either a single port number or a port range without gaps

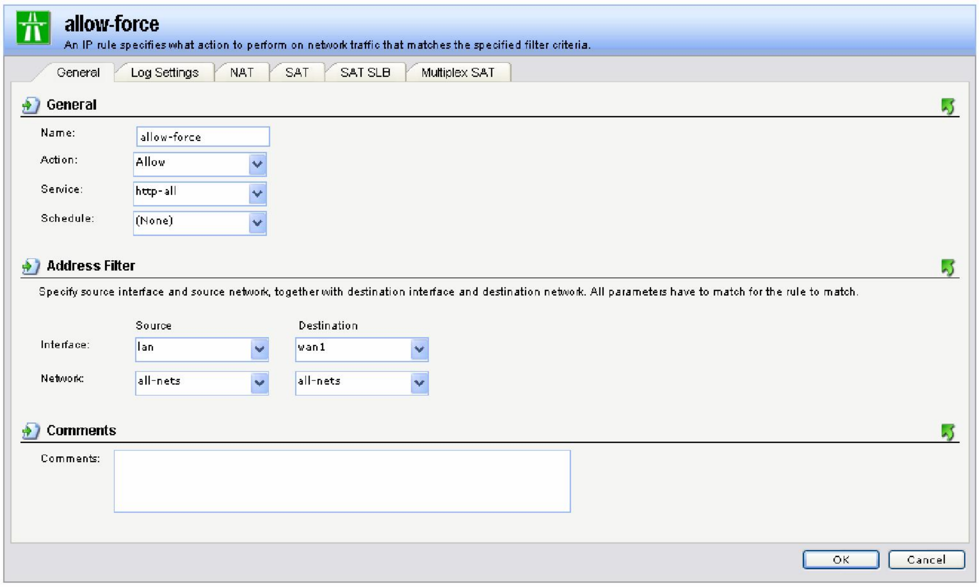
□ All-to-One Mapping: rewrite all destination IPs to a single IP

SAT:

Select **Destination IP Address** and in New IP Address select **lan-ip**

Click **Ok**.

Add another rule



allow-force

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

General

Name: allow-force

Action: Allow

Service: http-all

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	wan1
Network:	all-nets	all-nets

Comments

Comments:

General:

Name: **allow-force**
Action: **Allow**
Service: **http-all**

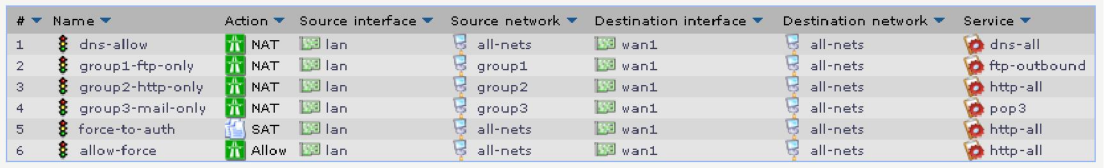
Source Interface: **lan**
Source Network: **all-nets**

Destination Interface: **wan1**
Destination Network: **all-nets**

You can enable Logging on this rule as well.

Then click **Ok**.

Once done you should see something like the below **(They need to be in the same order as below).**

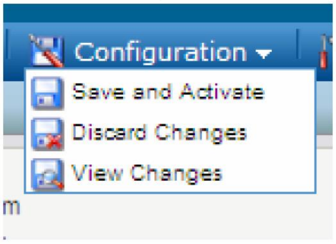


#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	dns-allow	NAT	lan	all-nets	wan1	all-nets	dns-all
2	group1-ftp-only	NAT	lan	group1	wan1	all-nets	ftp-outbound
3	group2-http-only	NAT	lan	group2	wan1	all-nets	http-all
4	group3-mail-only	NAT	lan	group3	wan1	all-nets	pop3
5	force-to-auth	SAT	lan	all-nets	wan1	all-nets	http-all
6	allow-force	Allow	lan	all-nets	wan1	all-nets	http-all

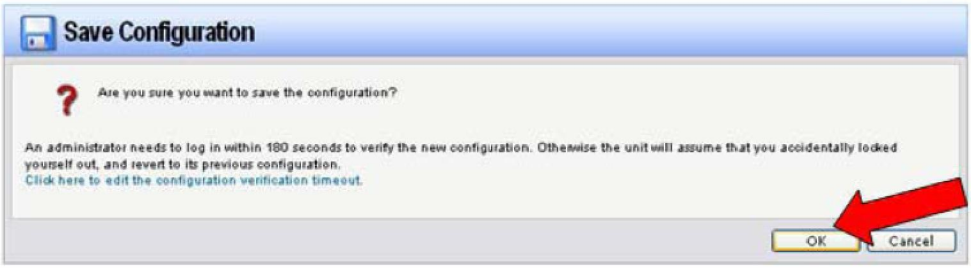
If the rules are not in the same order **right click** on the name of the one that is out of order and then you can select to **move up** or **move down**.

Step 5: Save Setting

Click **Configuration** then **Save and Activate**



Then click **Ok** once more the confirm to save the settings.



Are you sure you want to save the configuration?

An administrator needs to log in within 180 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.
Click here to edit the configuration verification timeout.

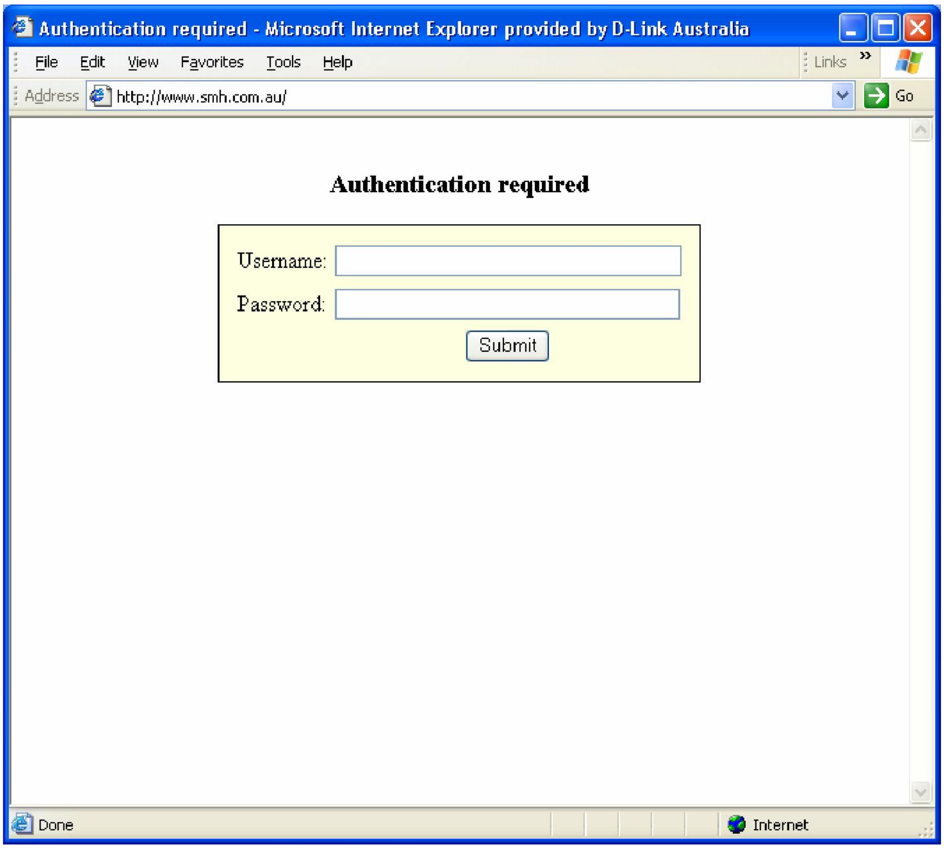
Wait around 15 seconds for the settings to be saved.

Once saved, try to access a web site.

You should get an **Authentication required** page. Enter in one of the username / passwords then click Submit, If the username you use has HTTP access the website should open.

To logout simple close the page.

Note: that if the user does not do anything for a period of time the login will time out (See step 4, Restrictions to change the time out).


Authentication required - Microsoft Internet Explorer provided by D-Link Australia
File
Edit
View
Favorites
Tools
Help
Links
Address
Go
Done
Internet

http://www.smh.com.au/

Authentication required

Username:

Password:

Submit