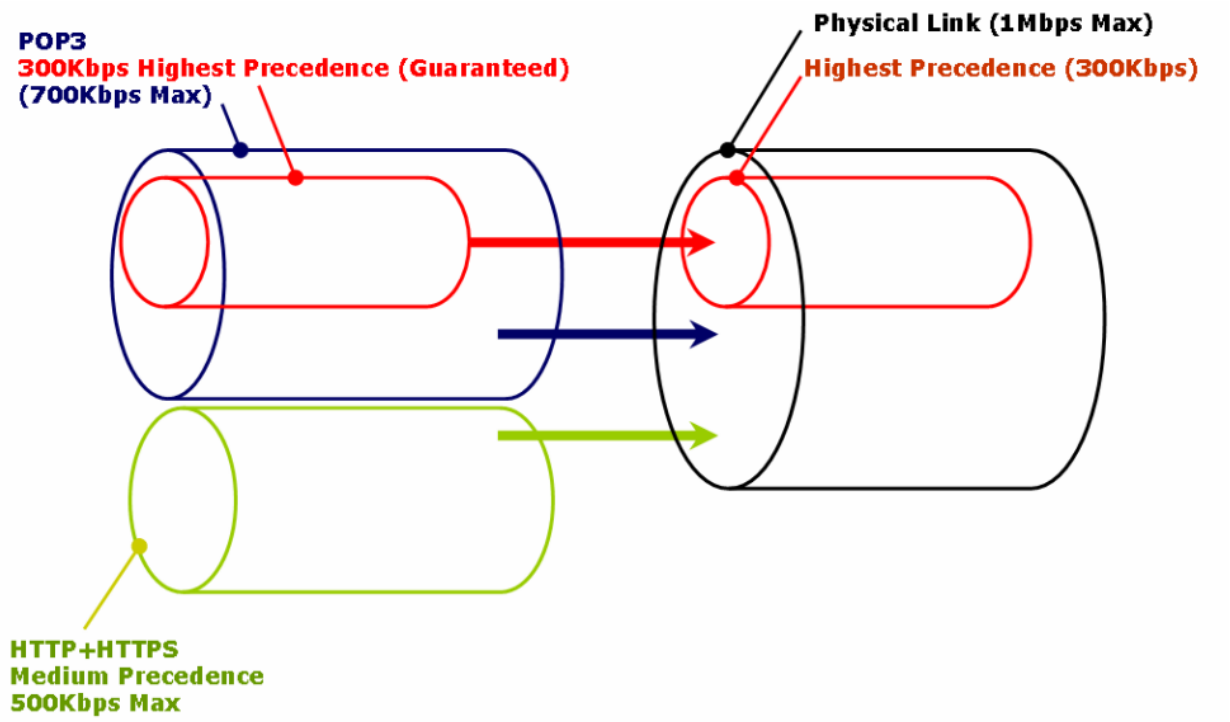
Configuration examples for the D-Link NetDefend Firewall series

How to setup traffic shaping

The below steps describe the configuration where we are using 1Mbps up / 1Mbps down link with the following traffic shaping rules:

- inbound and outbound HTTP and HTTPS the max bandwidth is 500Kbps.
- inbound and outbound POP3 the guaranteed bandwidth is 300Kbps, max is 700Kbps.
- other inbound and outbound services use the remaining bandwidth.

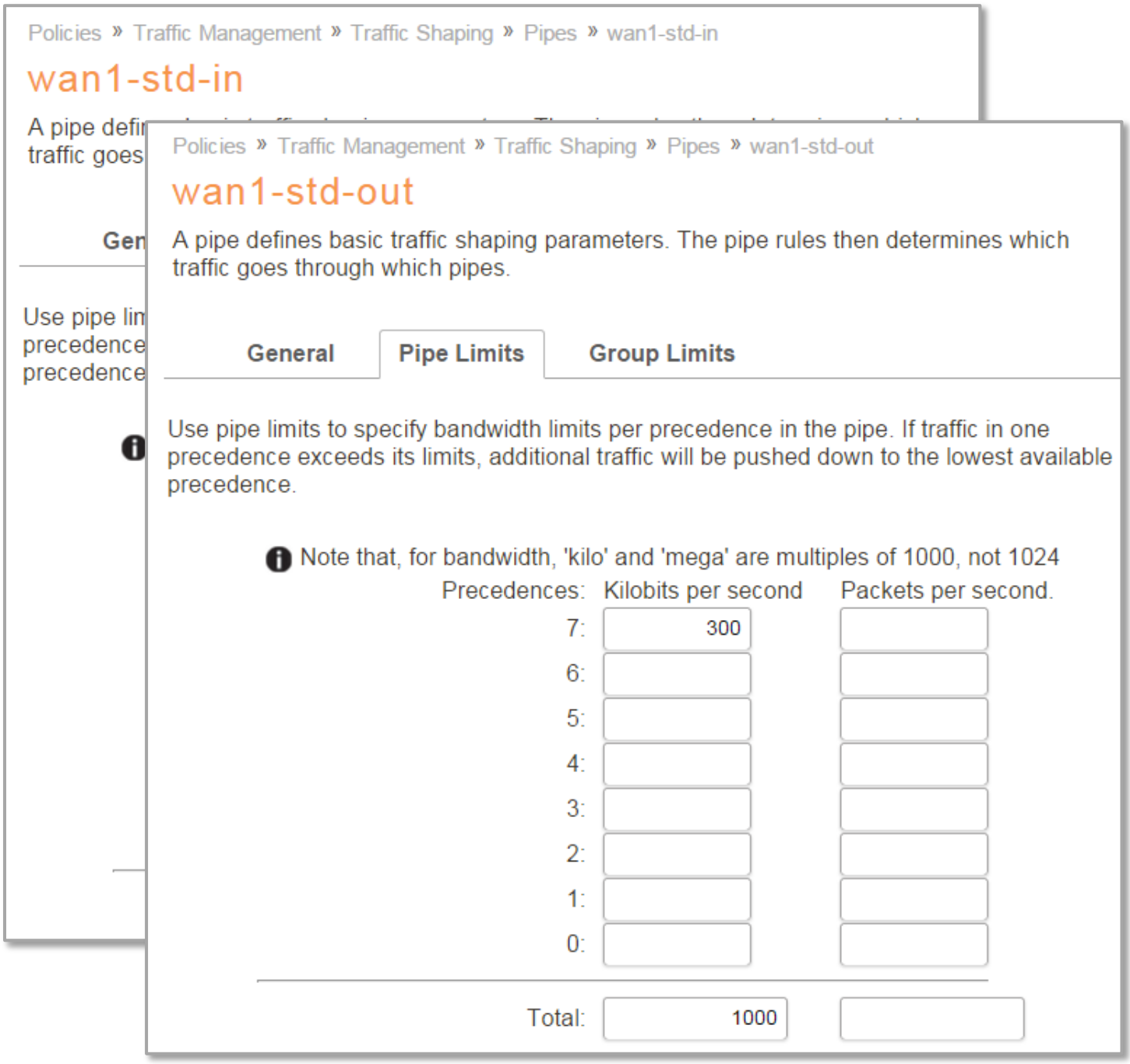
Here is the schematic representation of the three traffic shaping pipes we are going to create (we will need three pipes for outbound and three pipes for inbound traffic):



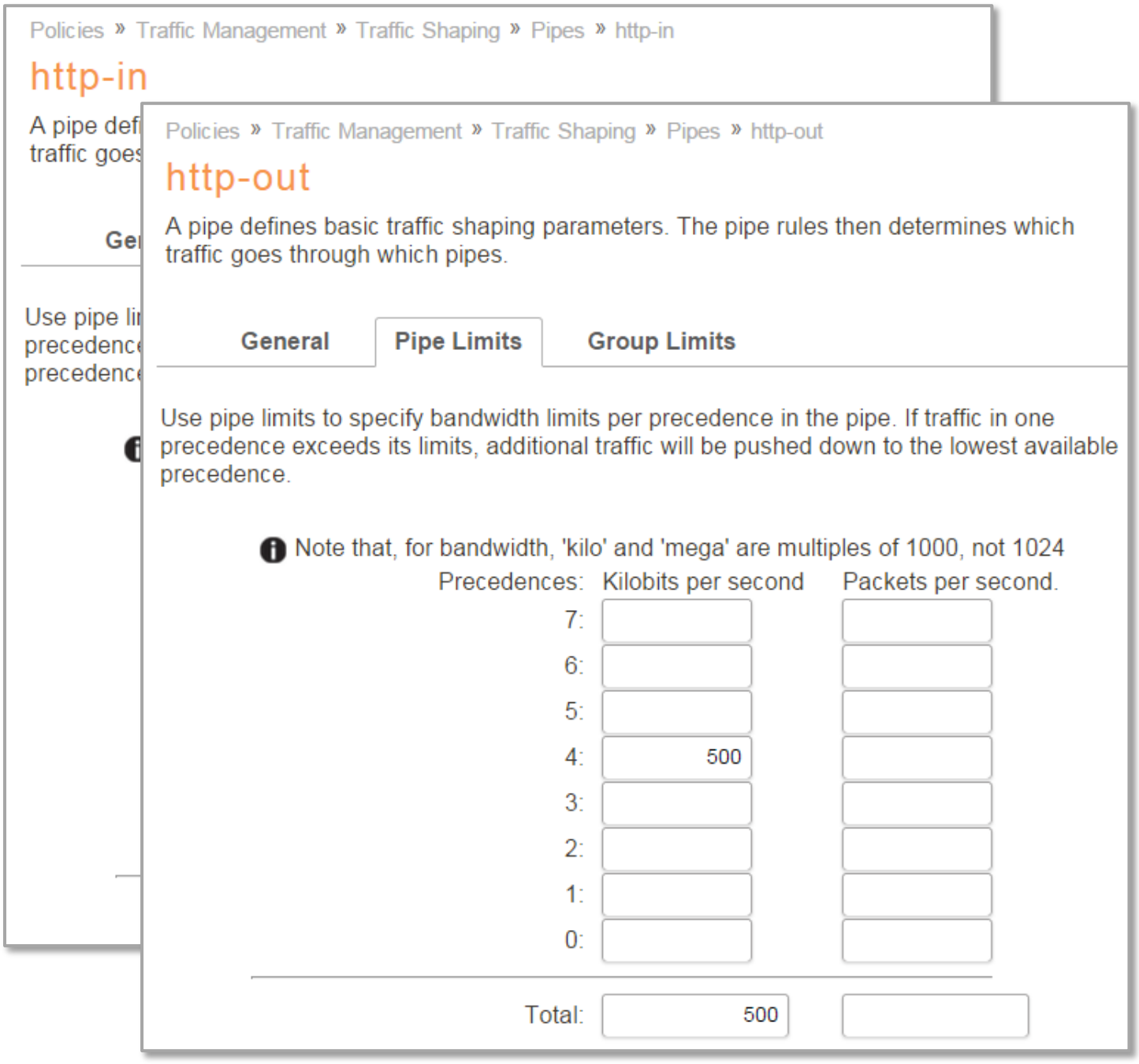
Step 1. Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is "admin" and password is "admin".

Step 2. Go to Policies > Traffic Management >Pipes.
Create a new entry for a “standard-in” pipe which describes physical connection limitations for download speed. Set the pipe limits: Total - 1000Kbps. Under Precedences set “7” with 300Kbps (this is for the guaranteed bandwidth).

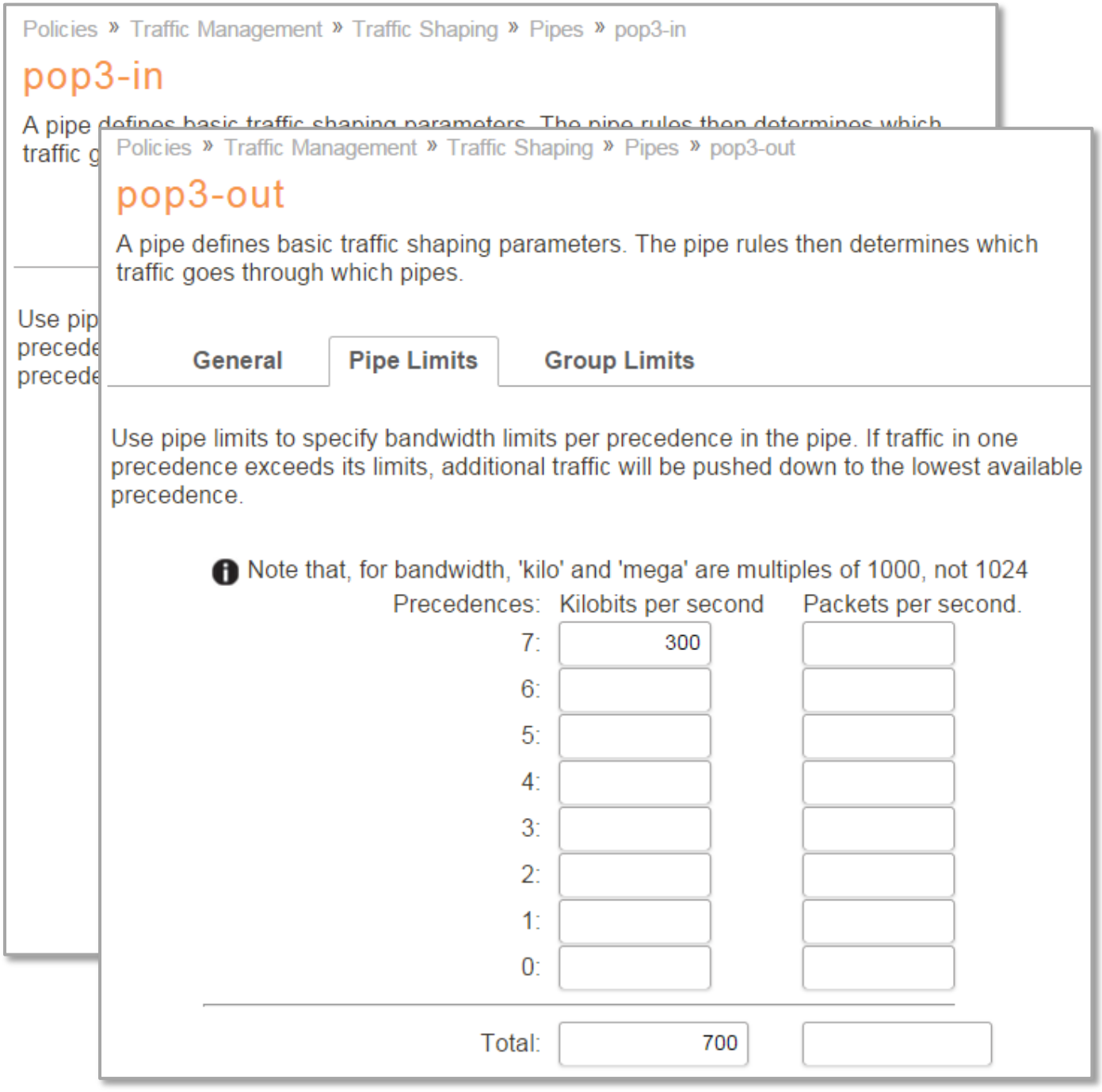
Create another pipe for “standard-out” (upload speed). Set the pipe limits: Total - 1000Kb. Under Precedences set “7” with 300Kbps.



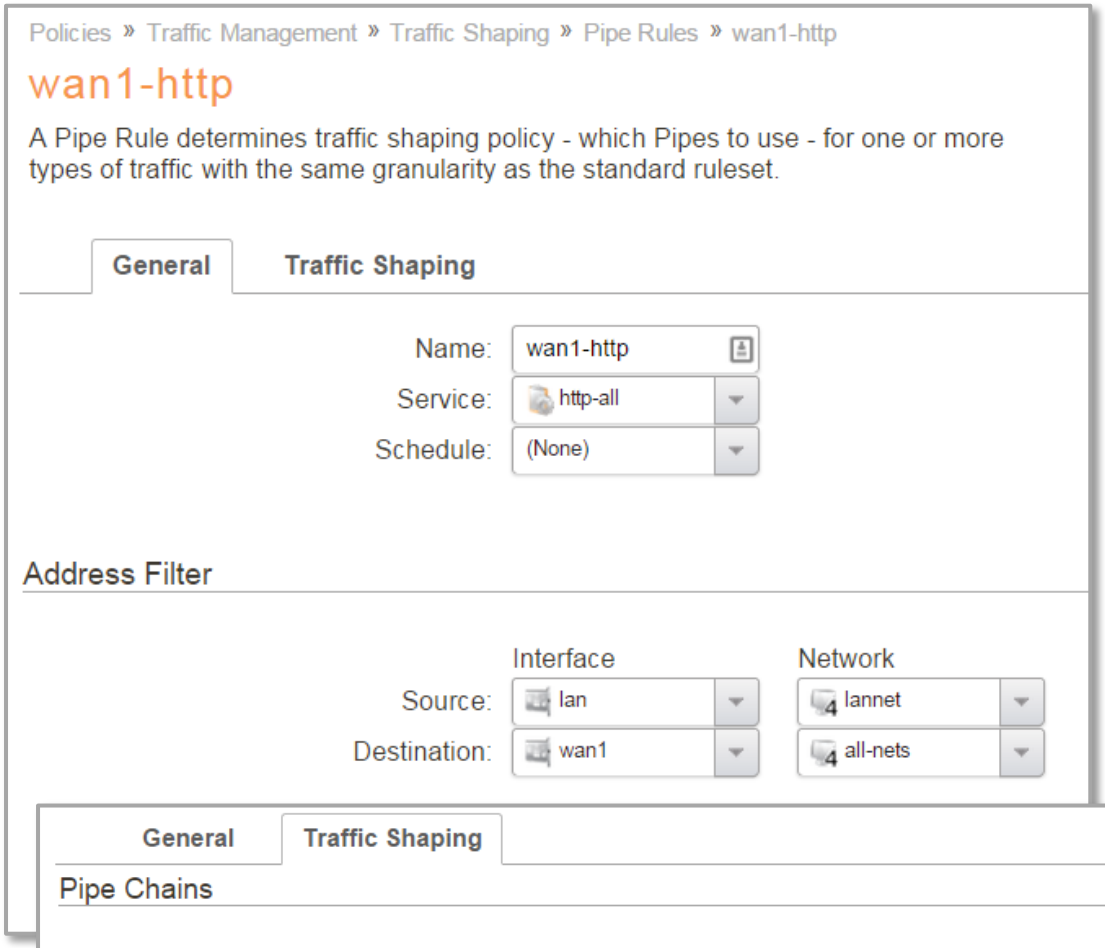
Step 3. Create two pipes (in and out) for HTTP traffic: Total bandwidth – 500 kbps. Precedence: “4” with 500 kbps limit.

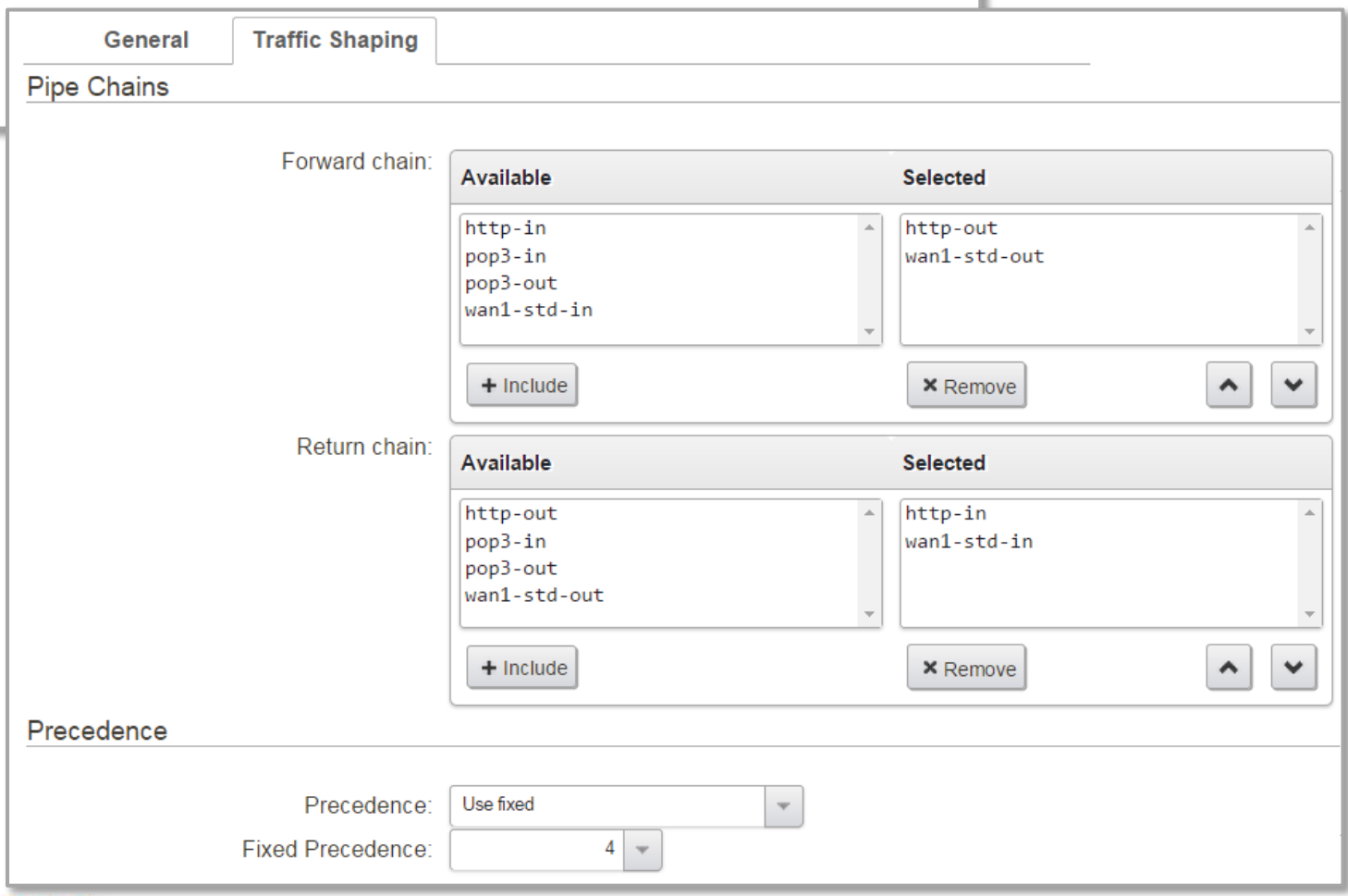


Step 4. Create two more pipes (in and out) for POP3 traffic: Total bandwidth – 700 kbps. Precedence: "7" with 300 kbps limit.

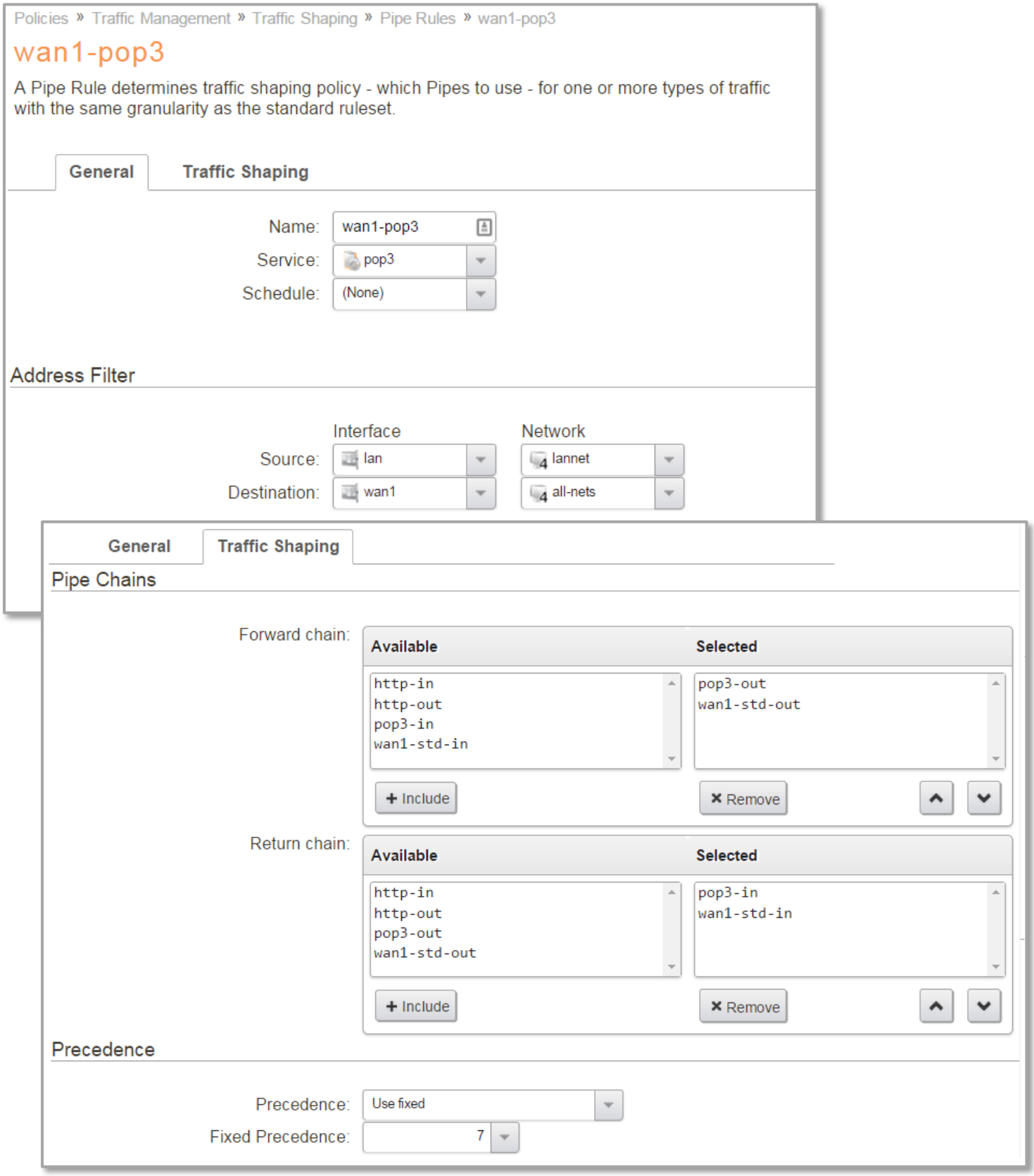


Step 5. Go to Policies > Traffic Management > Pipe Rules. You need to create Pipe Rules which would direct the selected traffic (HTTP or POP3) into specific pipe.
Create a Pipe Rule for HTTP traffic. Service - HTTP-All; Source LAN/LAN-Net; Destination - WAN/All-nets. Click on Traffic Shaping tab and add the pipes for outgoing traffic (Forward Chain - HTTP-out, Standard-out) and incoming traffic (Return Chain - HTTP-in, Standard-in). Set Precedence to “4”.

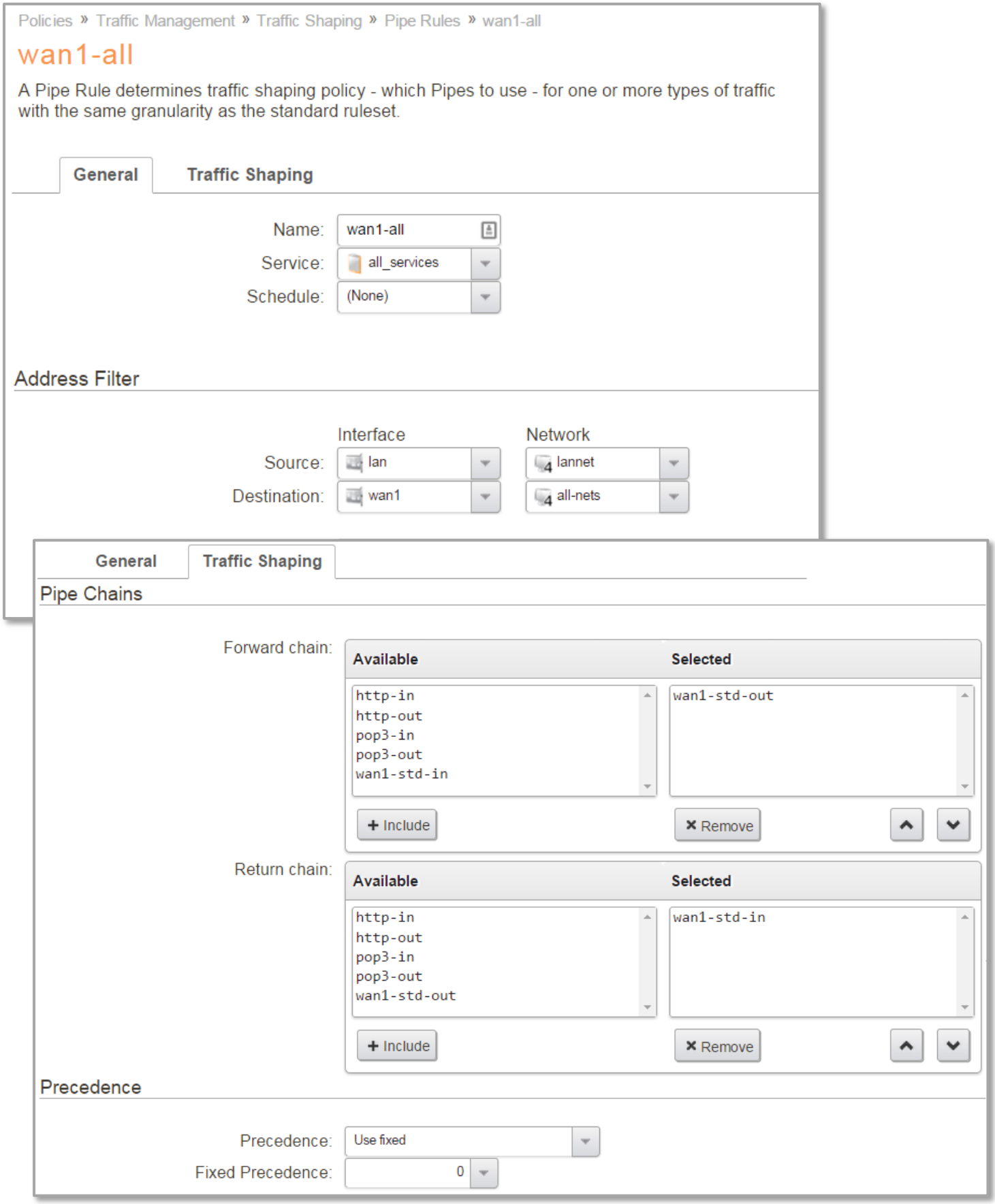




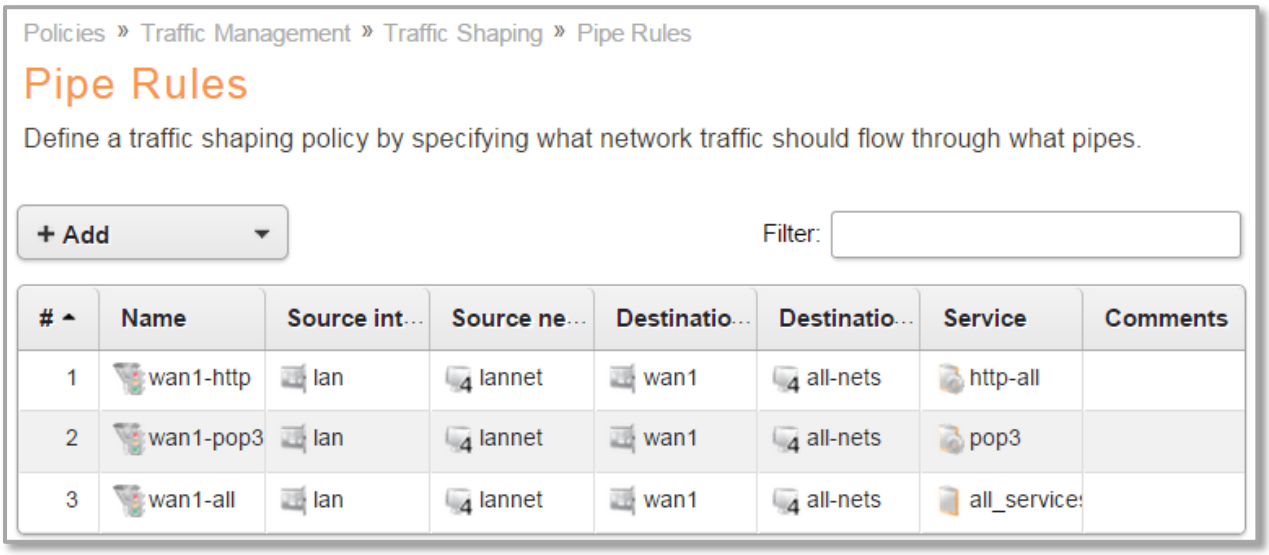
Step 6. Create a Pipe Rule for POP3 traffic. Service – POP3; Source LAN/LAN-Net; Destination - WAN/All-nets. Click on Traffic Shaping tab and add the pipes for outgoing traffic (Forward Chain – POP3-out, Standard-out) and incoming traffic (Return Chain – POP3-in, Standard-in). Set Precedence to “7”.



Step 7. Create another Pipe Rule for the rest of the services. Click on Traffic Shaping tab and add the pipes for outgoing traffic (Forward Chain - Standard-out) and incoming traffic (Return Chain - Standard-in). Set Precedence to ”0”.

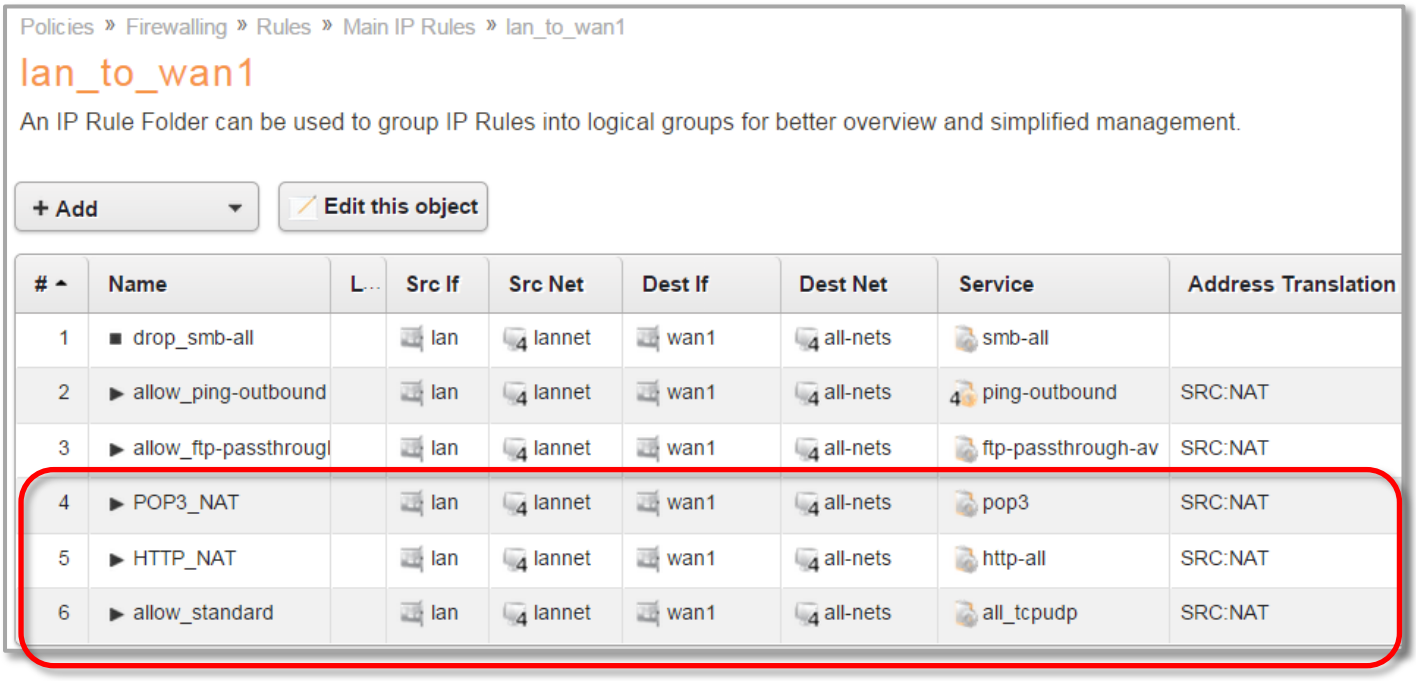


Make sure that the Pipe Rule for the rest of the traffic is positioned **after** the other rules.



Step 8. Go to Policies > Firewalling > Main IP Rules > "lan_to_wan". Create additional NAT rules for HTTP and POP3 traffic (you can "clone" the default "allow_standard" NAT rule and change "all_tcpudp" service to HTTP and POP3).

Make sure the new NAT rules are positioned above the "allow_standard" NAT rule.



Step 9. After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.