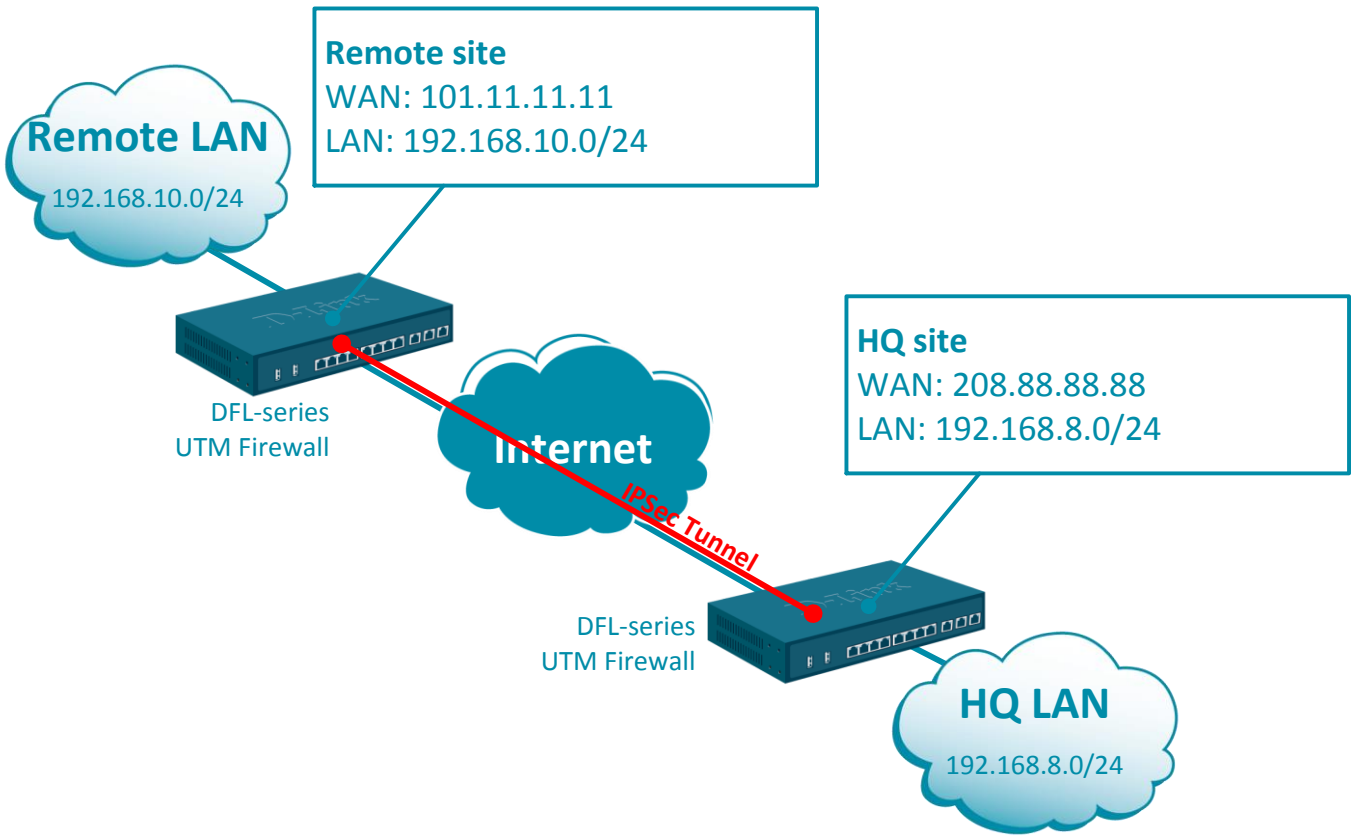
Configuration examples for the D-Link NetDefend Firewall series

Setting up IPsec VPN tunnel for site-to-site connection

This configuration example is based on the following setup:

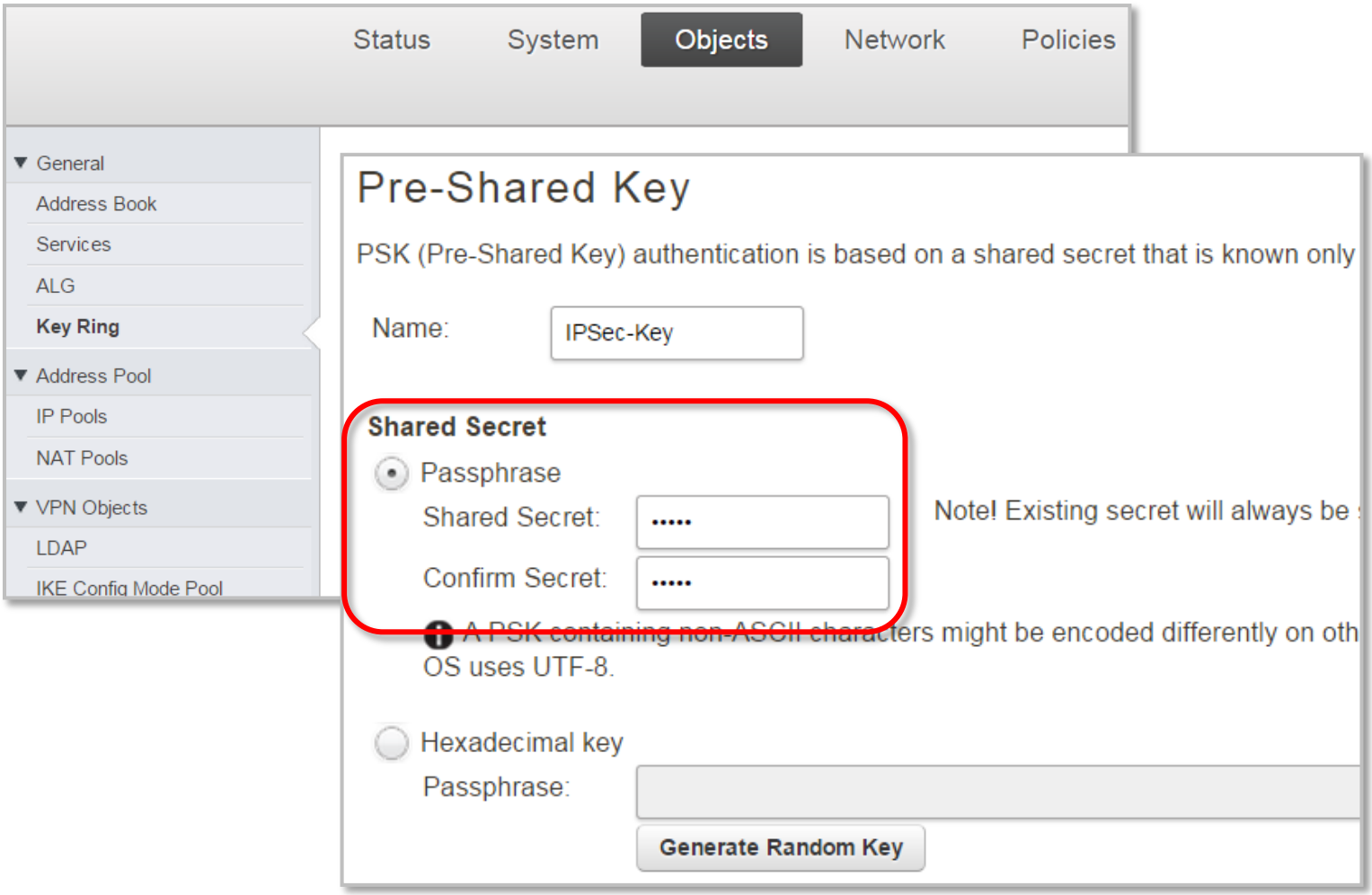


HQ site Firewall Configuration

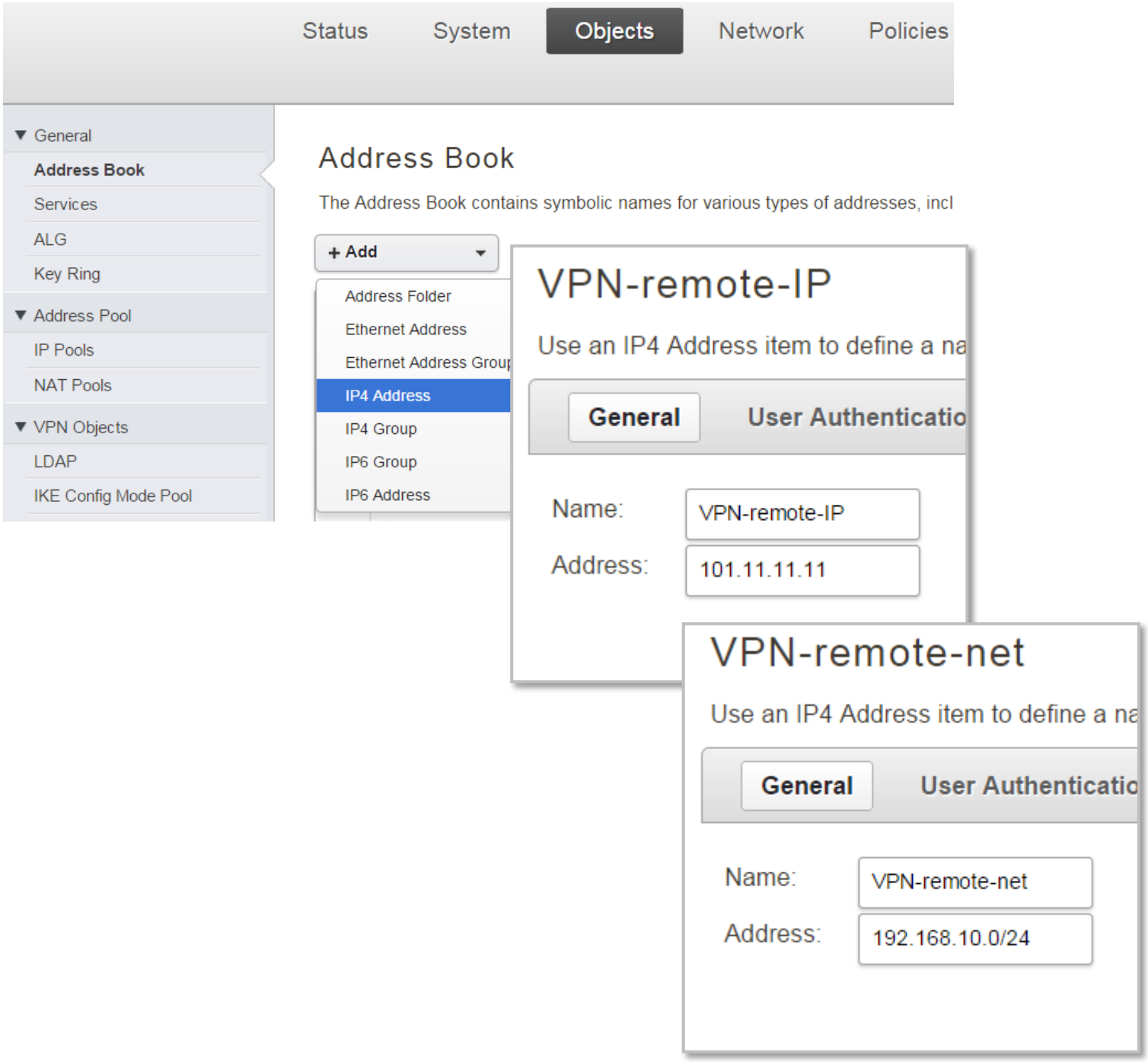
Step 1. Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is "admin" and password is "admin".

Step 2. Set your firewall's WAN settings as per Internet provider requirements.
In our example WAN is set with a static IP address.

Step 3. Go to Objects > Key Ring. Create a new Pre-Shared Key. The same key must be used on the remote VPN Firewall.

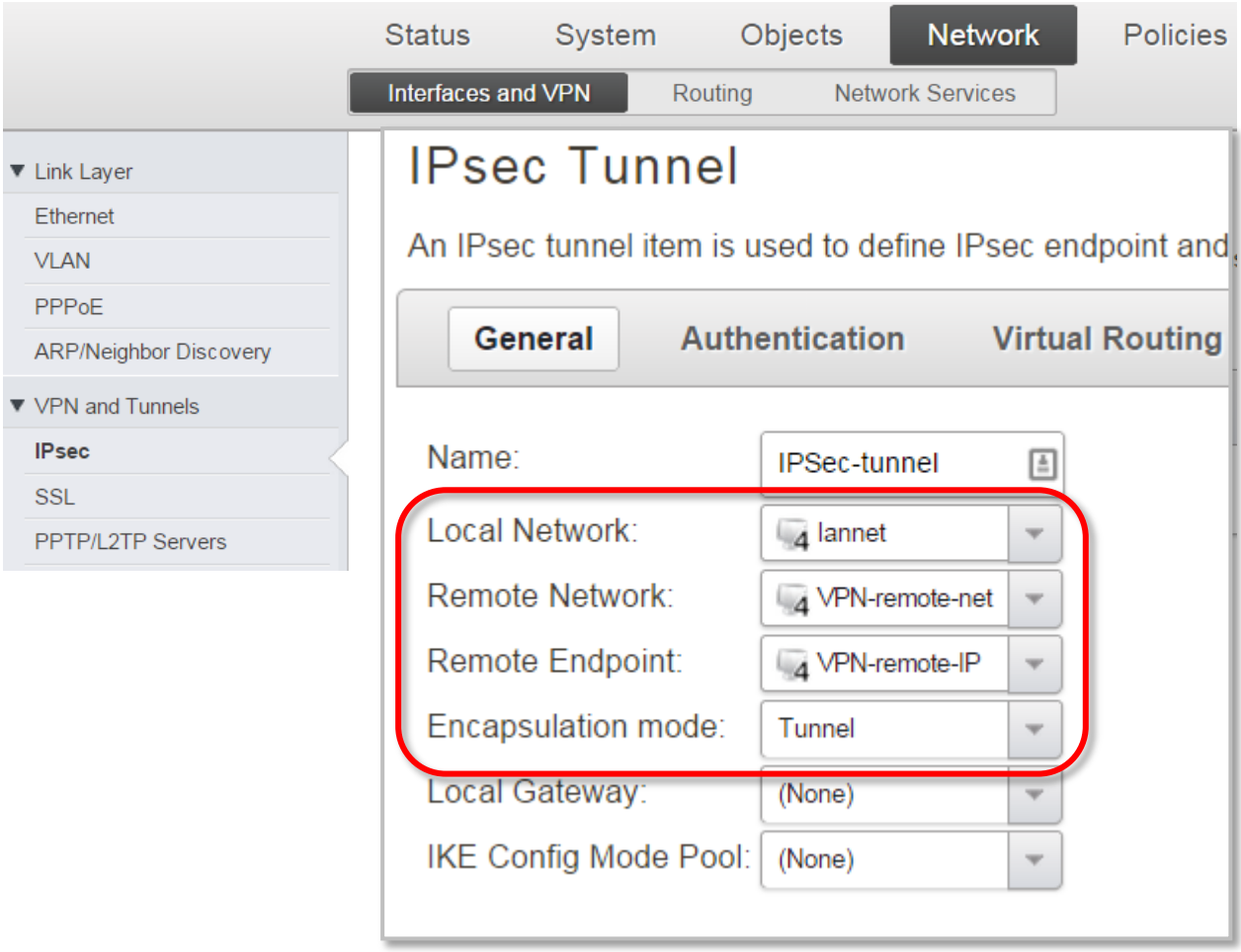


Step 4. Go to Objects > Address Book. Add two new objects for the remote network addresses: WAN IP of the remote VPN firewall (e.g. public IP) and the remote private LAN.

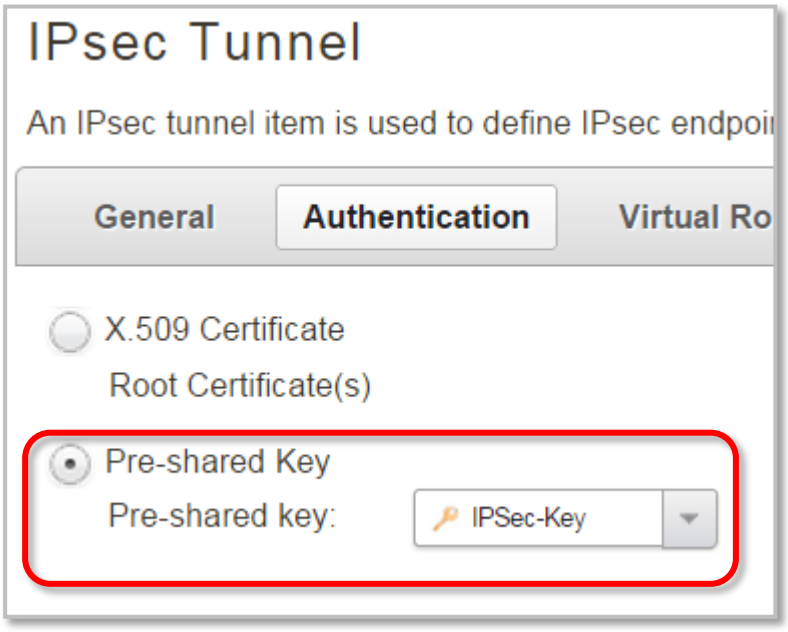


If you have multiple remote sites – create objects for all of them (remote public IP and remote network). Each of the remote sites needs to have a different network, e.g. 192.168.5.0/24, 192.168.6.0/24, etc.
If the public IP address on the remote site is dynamic you can utilize one of the Dynamic IP services. In this case your HQ firewall needs to use URL instead of IP address, following this format: *dns:myremotesite.dyndns.com*

Step 5. Go to Network > IPsec. Create a new tunnel and specify the remote network settings.



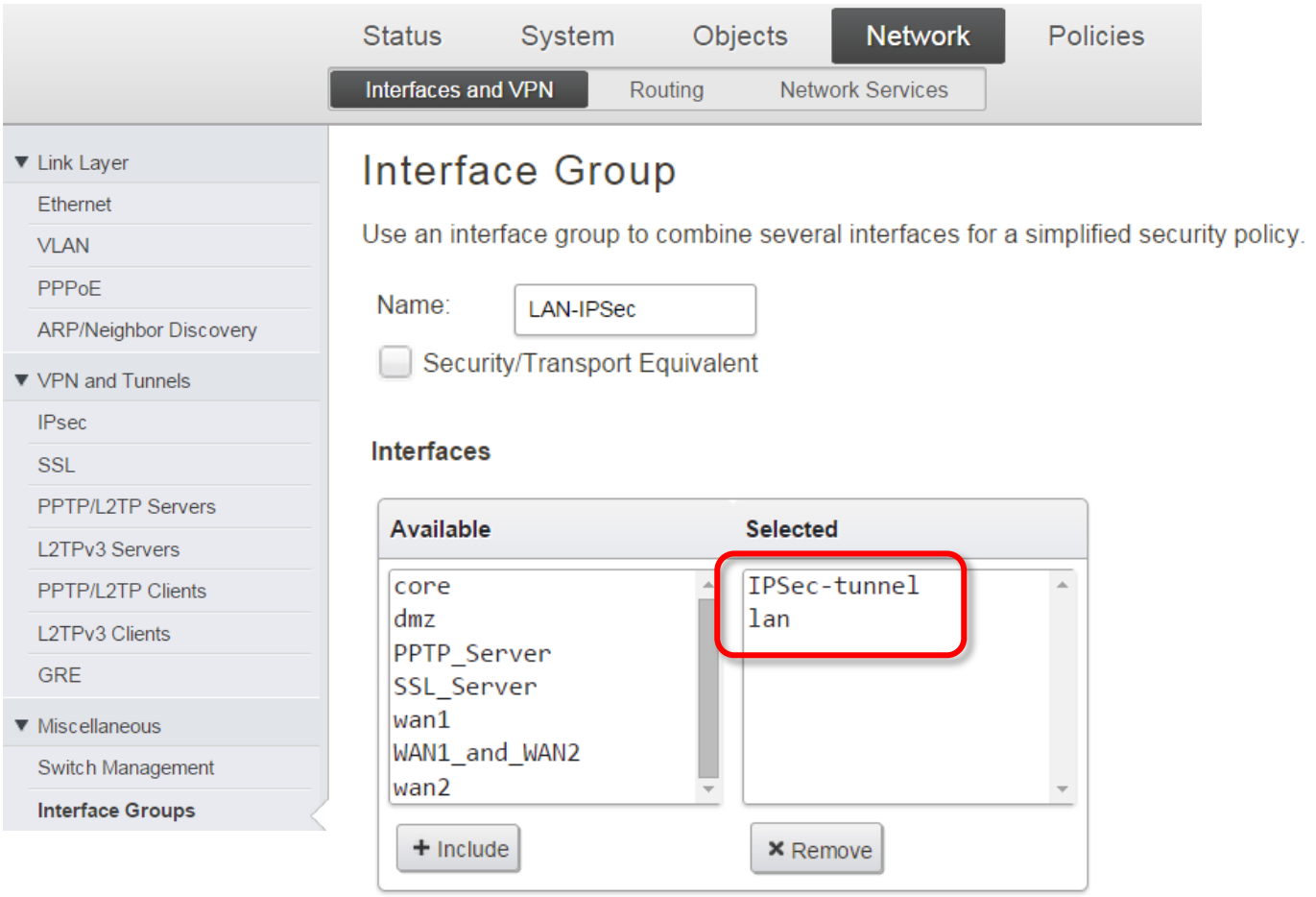
Click on Authentication tab and select the Pre-Shared Key you created on Step 3.



Note: If WAN port of the firewall is set with PPPoE authentication (default metric is 90), select the Advanced tab and change the Route Metric for the IPsec Tunnel to 80.

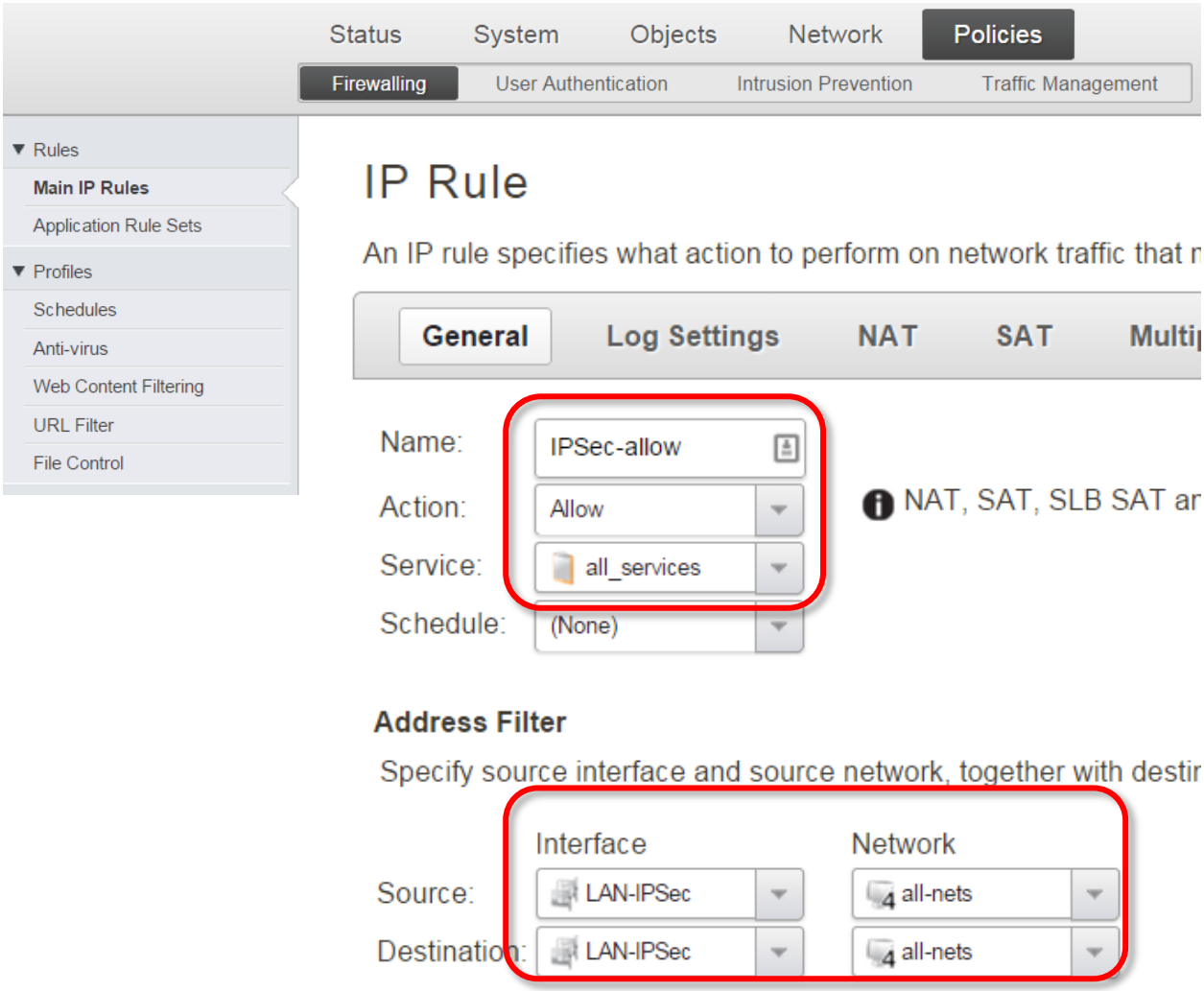
Create separate VPN tunnels for each of the remote sites you have (this is needed only on the firewall at HQ site).

Step 6. Go to Interfaces > Interface Groups. Create a new group and add the IPsec Tunnel and the LAN into the group (this is just to make it easier to apply rules to both interfaces in one go).



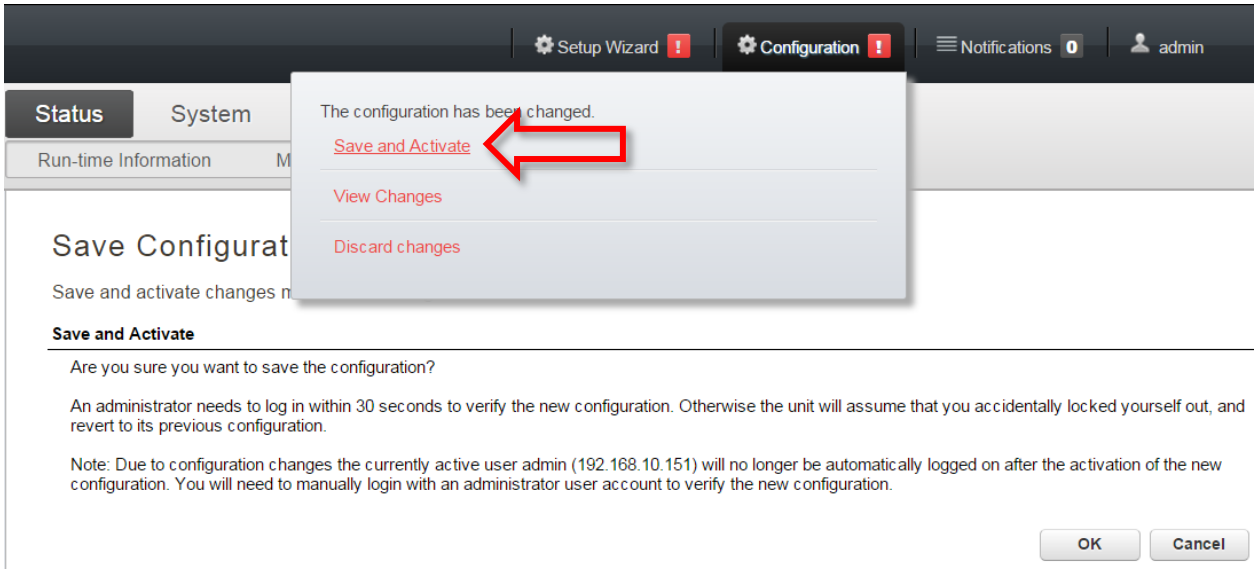
If you have multiple remote sites – add them all into this group.

Step 7. Go to Policies > Main IP Rules. Create a new rule to allow communication between LAN and the IPsec tunnel. Because we created the interface group "LAN-IPSec", this one rule will cover both IPsec Tunnel – to – LAN and LAN – to – IPsec Tunnel communication.



Step 8. 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.



Remote site Firewall Configuration

Repeat the steps above on the firewall at the remote sites. The only difference will be the IP addresses in “VPN-remote-IP” (in our example it is 208.88.88.88) and “VPN-remote-net” (in our example it is 192.168.8.0/24).