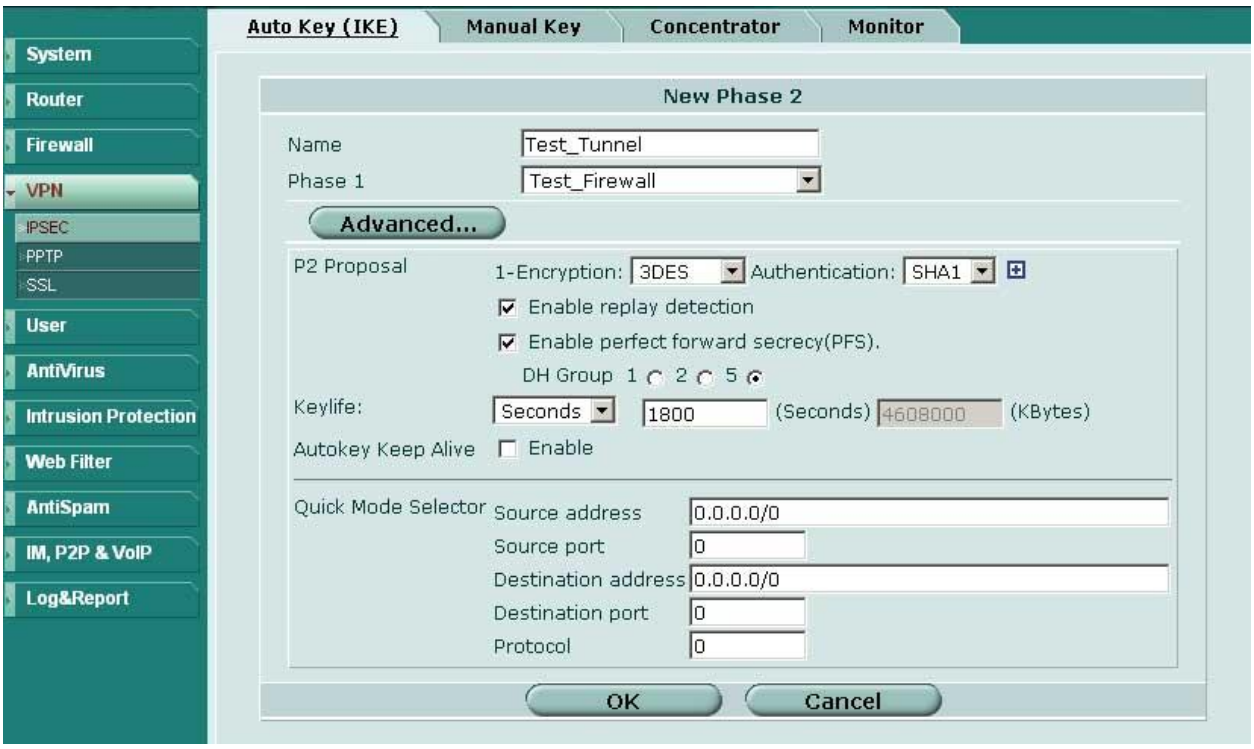
Dynamic Routing Protocols over IPSEC VPNs

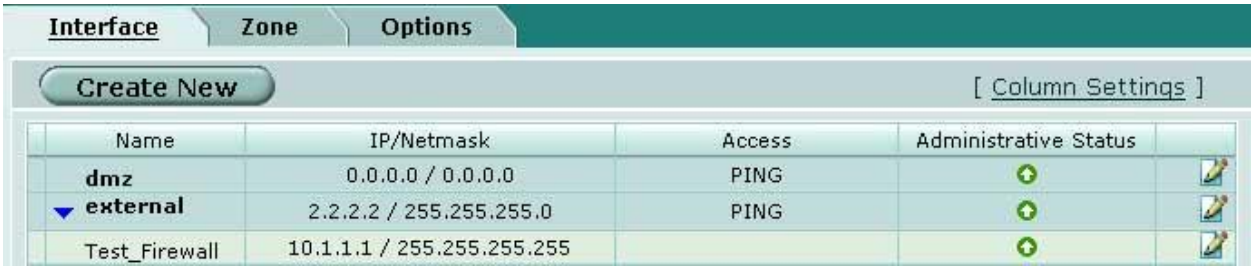
http://firewallguru.blogspot.com/2008/03/dynamic-routing-protocols-over-ipsec.html

This article describes how to configure dynamic routing protocols such as OSPF or BGP when using IPSEC VPNs. BGP is fairly easy since you define static neighbors. It does get a little more tricky when using multicast-based protocols such as OSPF. But despair not for help is nigh ;)

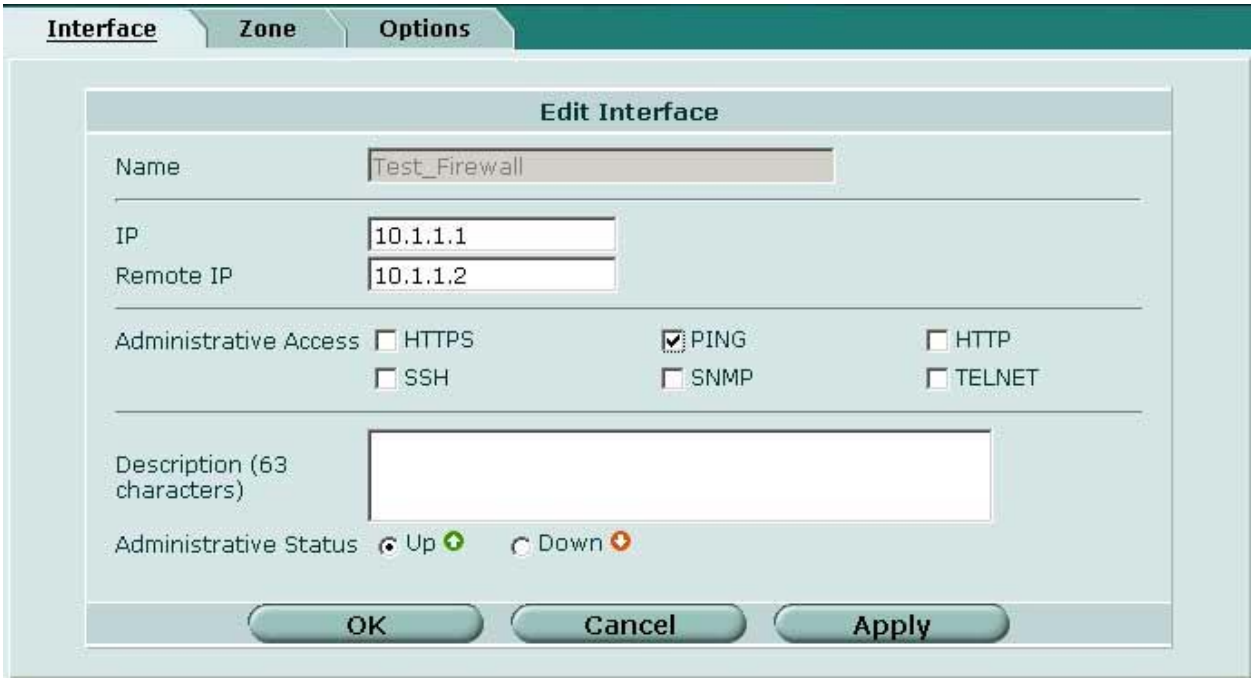
Start by building your site-to-site VPN tunnels in interface mode (see here for more info on interface mode). Important Note: Make sure your Phase 2 quick mode selectors are set to 0.0.0.0/0



Once you have your tunnels configured go to Network -> Interface and expand the blue triangle next to the interface to which you have the tunnel attached

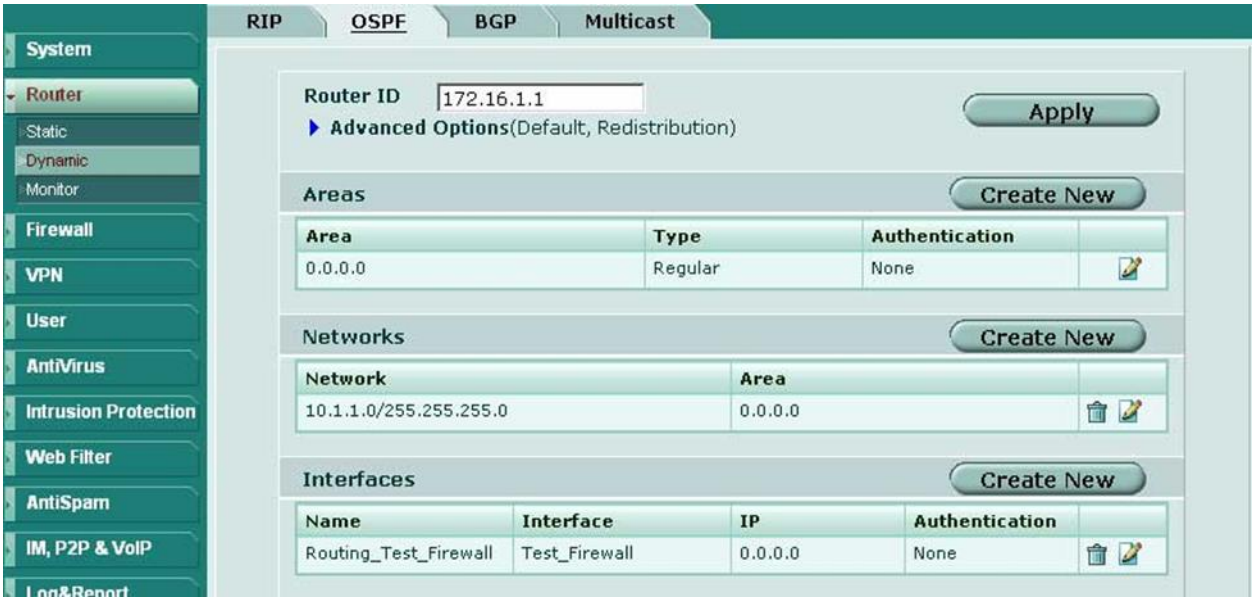


Something which is not immediately obvious is that you can define an IP address on the tunnel interface. Edit the tunnel interface and assign unique IP addresses (i.e. something that is not in use on your network, typically a private IP) for the local and remote IP:



On the other side of the tunnel perform the same operation, reversing the settings for local and remote IP

Now on to the OSPF side of things. Under Router -> Dynamic -> OSPF define Area 0.0.0.0 (the backbone). Then configure a Network which includes the network of the tunnel interface and place it in area 0.0.0.0. Under Interfaces create an interface tied to the tunnel interface. You can leave the IP as 0.0.0.0



Repeat the same on the other end and you should see your routes starting to come in as OSPF dynamic routes. To control which routes are advertised you can redistribute networks under the Advanced Options in OSPF. You can also apply router access lists to filter networks from being advertised. More on router access lists (used for OSPF) and router prefix lists (used for BGP) in another post