

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

System
Router
Firewall
VPN
IPSEC
PPTP
SSL
User
AntiVirus
Intrusion Protection
Web Filter
AntiSpam
IM, P2P & VoIP
Log&Report

Auto Key (IKE) Manual Key Concentrator Monitor

New Phase 2

Name: Test_Tunnel
Phase 1: Test_Firewall

Advanced...

P2 Proposal
1-Encryption: 3DES Authentication: SHA1
 Enable replay detection
 Enable perfect forward secrecy(PFS).
DH Group: 1 2 5

Keylife: Seconds 1800 (Seconds) 4608000 (KBytes)
Autokey Keep Alive Enable

Quick Mode Selector
Source address: 0.0.0.0/0
Source port: 0
Destination address: 0.0.0.0/0
Destination port: 0
Protocol: 0

OK Cancel

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

Interface Zone Options

Create New [Column Settings]

Name	IP/Netmask	Access	Administrative Status
dmz	0.0.0.0 / 0.0.0.0	PING	
external	2.2.2.2 / 255.255.255.0	PING	
Test_Firewall	10.1.1.1 / 255.255.255.255	PING	

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:

The screenshot shows the 'Edit Interface' configuration window. The 'Interface' tab is selected. The 'Name' field contains 'Test_Firewall'. The 'IP' field contains '10.1.1.1' and the 'Remote IP' field contains '10.1.1.2'. Under 'Administrative Access', the 'PING' checkbox is checked, while 'HTTPS', 'SSH', 'HTTP', and 'TELNET' are unchecked. The 'Description' field is empty. The 'Administrative Status' is set to 'Up'. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

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

RIP **OSPF** BGP Multicast

System

Router

Static

Dynamic

Monitor

Firewall

VPN

User

AntiVirus

Intrusion Protection

Web Filter

AntiSpam

IM, P2P & VoIP

Log&Report

Router ID: 172.16.1.1 Apply

▶ **Advanced Options**(Default, Redistribution)

Areas Create New

Area	Type	Authentication	
0.0.0.0	Regular	None	

Networks Create New

Network	Area	
10.1.1.0/255.255.255.0	0.0.0.0	

Interfaces Create New

Name	Interface	IP	Authentication	
Routing_Test_Firewall	Test_Firewall	0.0.0.0	None	

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