Configuring route based IPSec using OSPF

August 2010

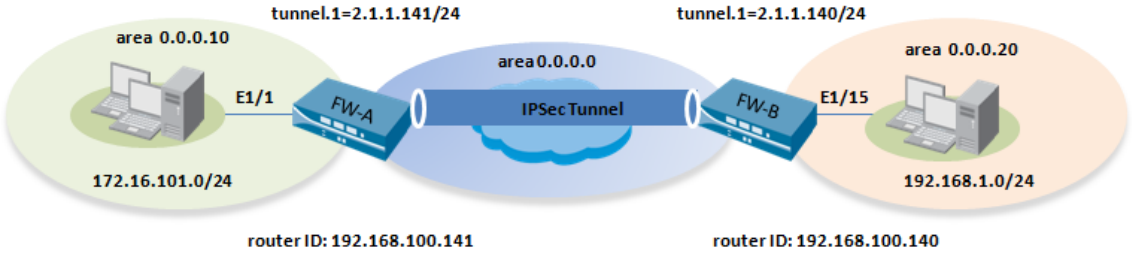
Palo Alto Networks
232 E. Java Dr.
Sunnyvale, CA 94089
408.738.7700
www.paloaltonetworks.com

Table of Contents

Overview

This document provides the configuration steps required to setup a route based IPSec tunnel using OSPF.

Topology



The tunnel interface on both the firewalls is assigned to the OSPF backbone area, area 0.

Configuration on FW-A

For the sake of simplicity the relevant sections of the show commands are captured in this document. These sections can be combined to build the full configuration. Wherever applicable the webui screenshots are used for configuration

Interface configuration

```
admin@FW-A# show network interface ethernet ethernet1/1
ethernet1/1 {
  link-speed auto;
  link-duplex auto;
  link-state auto;
  layer3 {
    mtu 1500;
    ip {
      172.16.101.1/24;
    }
  }
}
[edit]
admin@FW-A# show network interface ethernet ethernet1/2
ethernet1/2 {
  link-speed auto;
  link-duplex auto;
```

```
  link-state auto;
  layer3 {
    mtu 1500;
    ip {
      100.1.1.1/24;

    }
  }
```

```
admin@FW-A# show network interface tunnel
tunnel {
  units {
    tunnel.1 {
      mtu 1400;
      ip {
        2.1.1.141/24;
      }
```

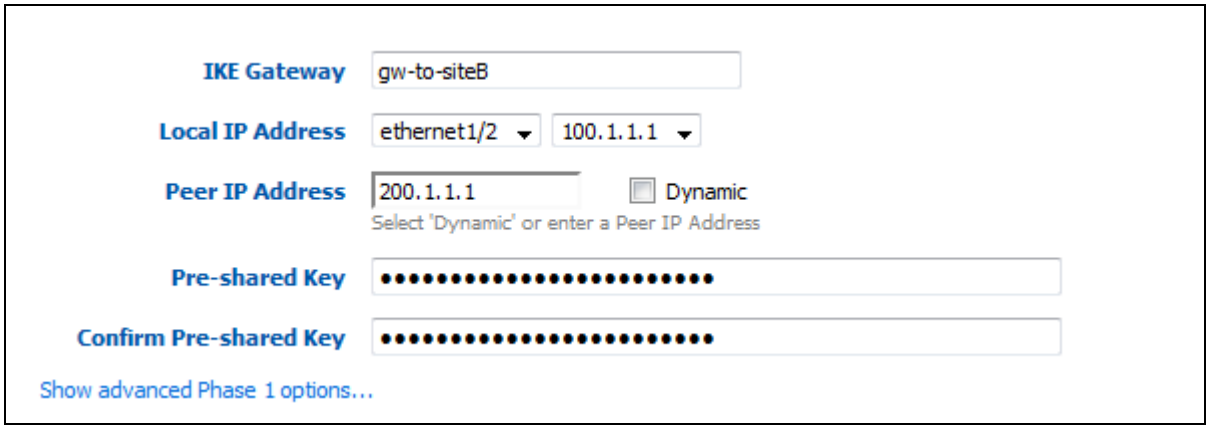
Zone configuration

Zones

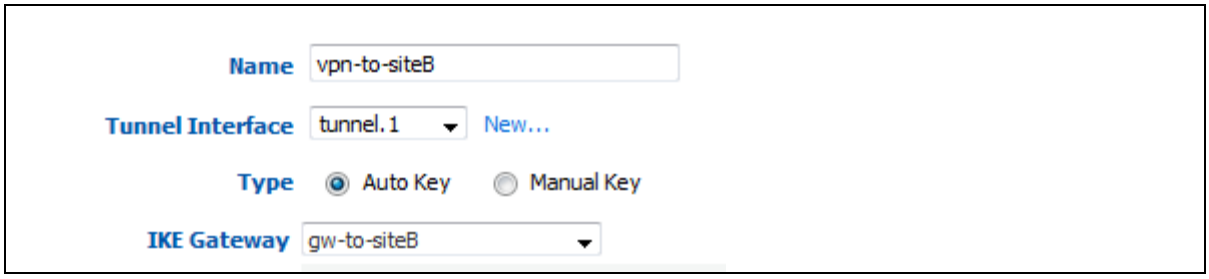
	Name	Type	Interfaces / Virtual Systems
☐	L2trust	layer2	
☐	L2Untrust	layer2	
☐	trust	layer3	ethernet1/1
☐	untrust	layer3	ethernet1/2
☐	VPN	layer3	tunnel.1
☐	vw-trust	virtual-wire	ethernet1/3 ethernet1/4

IKE and IPSec configuration

Network>network profiles> IKE gateways



Network>IPSec tunnels



Security policy

Security policies are required from the trust zone to the zone where the tunnel interface is bound to. In our example the following security policy is required

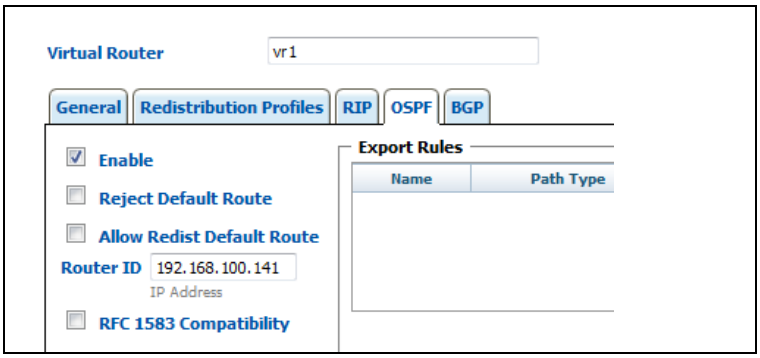
Source Zone	Destination Zone	Source IP	Destination IP	Application	Action
trust	vpn	172.16.101.0/24	192.168.1.0/24	any	allow

To allow bidirectional communication a policy in the reverse direction must be created

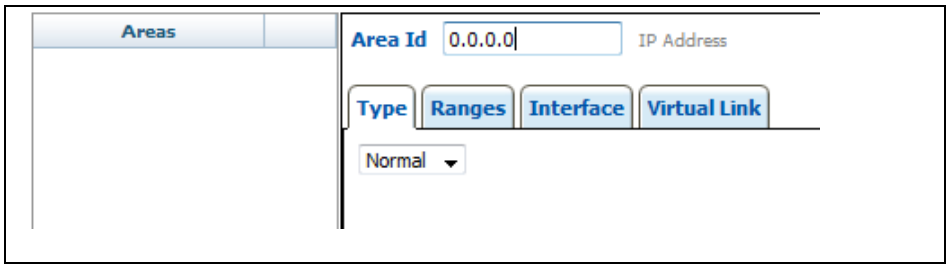
Source Zone	Destination Zone	Source IP	Destination IP	Application	Action
vpn	trust	192.168.1.0/24	172.16.101.0/24	any	allow

OSPF configuration

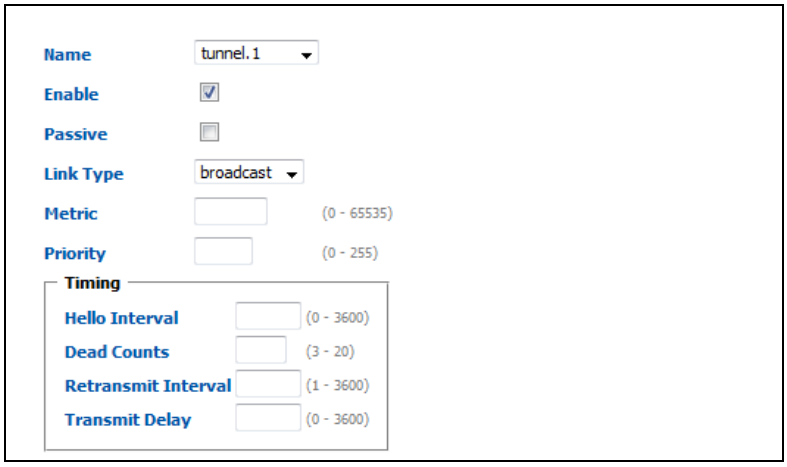
1. Go to ***Networks>Virtual Routers*** and select the virtual router on which OSPF will be enabled. Select the OSPF tab from the screen and check the box to enabled OSPF and assign a router ID.



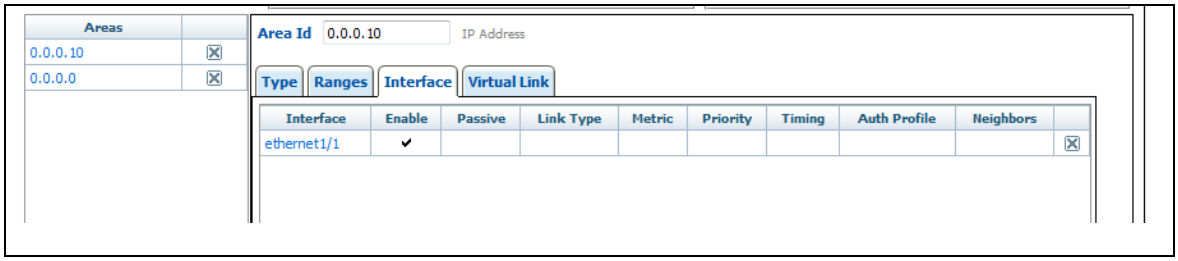
2. Click on **New** under the areas to create a new area. In the new area screen, enter the Area Id. For area 0, enter 0.0.0.0. Set the type of area to normal.



3. Click on the interface tab and choose tunnel.1 interface and click on add. The default metric is 1 and the link type is broadcast. For a site to site tunnel you can set the link type to p2p



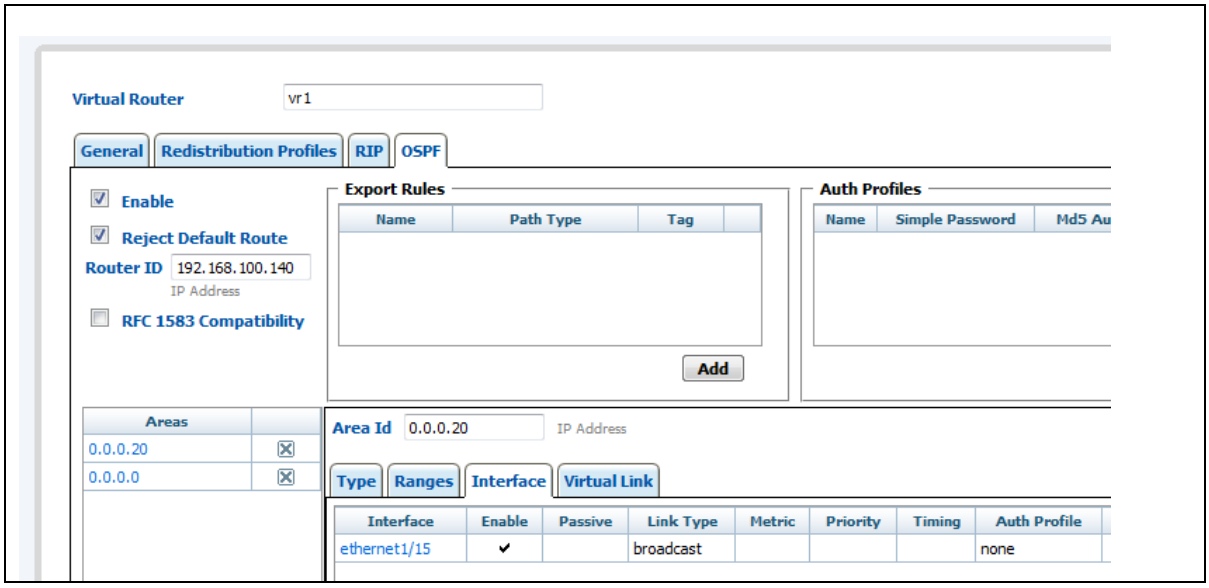
4. Create another area, area 10 and assign the interface ethernet1/1 to this area. The area id for area 10 must be entered as 0.0.0.10.



Configuration on FW-B

OSPF configuration

Repeat the OSPF configuration on FW-A, with the exception of creating area 20.



Verification

Verifying OSPF adjacencies

Both the firewalls must see each other as the neighbor with the FULL status. The neighbor address will be the IP address of the peer device's tunnel interface. Neighbor router ID is the IP address defined when configuring OSPF in step.

```
admin@FW-A>
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

```
admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

Verifying routes

The remote LAN network will be learned via OSPF with the tunnel interface as the nexthop

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination               nexthop              metric flags      age   interface          next-AS
2.1.1.0/24                0.0.0.0                  10   Oi       6760  tunnel.1
172.16.101.0/24           0.0.0.0                  10   Oi       6854  ethernet1/1
192.168.1.0/24            2.1.1.140                20 A Oo       6754  tunnel.1
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination               nexthop              metric flags      age   interface
2.1.1.0/24                0.0.0.0              10      Oi        20033 tunnel.1
172.16.101.0/24           2.1.1.141            20     AOo        6896  tunnel.1
192.168.1.0/24            0.0.0.0              10      Oi        8058  ethernet1/15
total routes shown: 3
```

Verifying the IPSec tunnel

```
admin@FW-A> show vpn flow

--------------------------------------------------------------------------------
total tunnels configured:           1
filter - type IPSec, state any


total IPSec tunnel configured:    1
total IPSec tunnel shown:         1

name                  id    state    local-ip        peer-ip         tunnel-i/f
--------------------------------------------------------------------------------
vpn-to-siteB:test     5     active   100.1.1.1       200.1.1.1       tunnel.1
--------------------------------------------------------------------------------
```