



# Configuring route based IPSec using OSPF

August 2010

Palo Alto Networks  
232 E. Java Dr.  
Sunnyvale, CA 94089  
408.738.7700  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

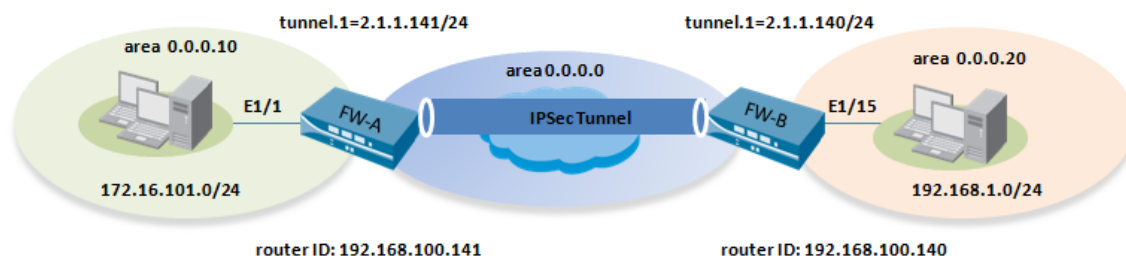
## Table of Contents

|                                      |   |
|--------------------------------------|---|
| Overview .....                       | 3 |
| Topology.....                        | 3 |
| Configuration on FW-A .....          | 3 |
| Configure IPSec.....                 | 4 |
| OSPF configuration.....              | 6 |
| Configuration on FW-B .....          | 7 |
| OSPF configuration.....              | 7 |
| Verification .....                   | 8 |
| Verifying the OSPF adjacencies ..... | 8 |
| Verifying the routes .....           | 9 |

## 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 |
| <input type="checkbox"/> | L2trust   | layer2       |                              |
| <input type="checkbox"/> | L2Untrust | layer2       |                              |
| <input type="checkbox"/> | trust     | layer3       | ethernet1/1                  |
| <input type="checkbox"/> | untrust   | layer3       | ethernet1/2                  |
| <input type="checkbox"/> | VPN       | layer3       | tunnel.1                     |
| <input type="checkbox"/> | vw-trust  | virtual-wire | ethernet1/3<br>ethernet1/4   |

## IKE and IPSec configuration

Network > network profiles > IKE gateways

**IKE Gateway**

**Local IP Address**

**Peer IP Address**   Dynamic  
Select 'Dynamic' or enter a Peer IP Address

**Pre-shared Key**

**Confirm Pre-shared Key**

[Show advanced Phase 1 options...](#)

Network > IPSec tunnels

**Name**

**Tunnel Interface**  [New...](#)

**Type**  Auto Key  Manual Key

**IKE Gateway**

## 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

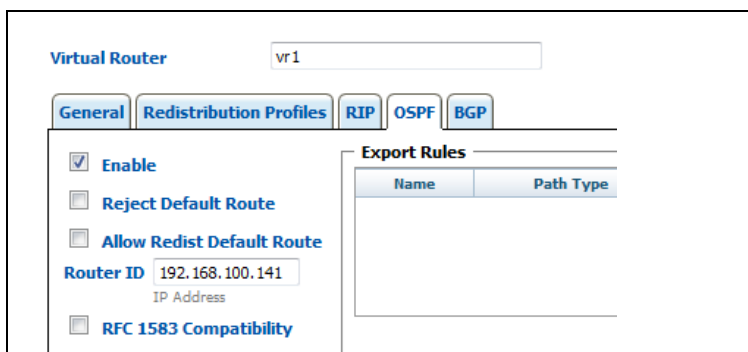
| Source Zone | Destination Zone | Source IP       | Destination IP | Application | Action |
|-------------|------------------|-----------------|----------------|-------------|--------|
| trust       | vpn              | 172.16.101.0/24 | 192.168.1.0/24 | any         | allow  |

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  |

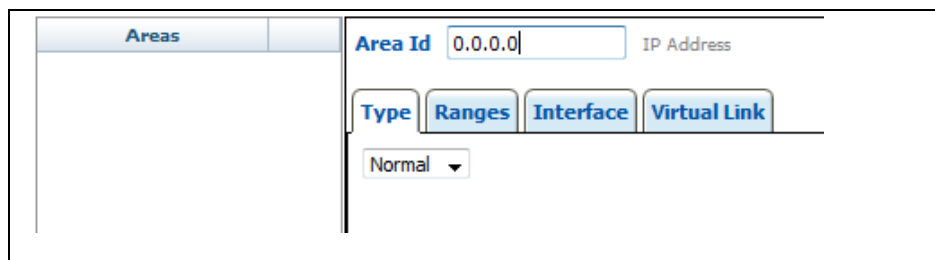
## OSPF configuration

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.



The screenshot shows the configuration page for a virtual router named 'vr1'. The 'OSPF' tab is selected. The 'Enable' checkbox is checked. The 'Router ID' is set to '192.168.100.141'. The 'Export Rules' section is empty.

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.



The screenshot shows the configuration page for a new area. The 'Area Id' is set to '0.0.0.0'. The 'Type' is set 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

**Name**

**Enable**

**Passive**

**Link Type**

**Metric**  (0 - 65535)

**Priority**  (0 - 255)

**Timing**

**Hello Interval**  (0 - 3600)

**Dead Counts**  (3 - 20)

**Retransmit Interval**  (1 - 3600)

**Transmit Delay**  (0 - 3600)

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.

| Areas    |                                     | Area Id  | IP Address |
|----------|-------------------------------------|----------|------------|
| 0.0.0.10 | <input checked="" type="checkbox"/> | 0.0.0.10 |            |
| 0.0.0.0  | <input checked="" type="checkbox"/> |          |            |

| Type        |                                     | Ranges  |           | Interface |          | Virtual Link |              |                                     |
|-------------|-------------------------------------|---------|-----------|-----------|----------|--------------|--------------|-------------------------------------|
| Interface   | Enable                              | Passive | Link Type | Metric    | Priority | Timing       | Auth Profile | Neighbors                           |
| ethernet1/1 | <input checked="" type="checkbox"/> |         |           |           |          |              |              | <input checked="" type="checkbox"/> |

## *Configuration on FW-B*

### *OSPF configuration*

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

Virtual Router

Enable  
 Reject Default Route  
 Router ID   
IP Address  
 RFC 1583 Compatibility

**Export Rules**  

| Name | Path Type | Tag |
|------|-----------|-----|
| Add  |           |     |

**Auth Profiles**  

| Name | Simple Password | Md5 Au |
|------|-----------------|--------|
| Add  |                 |        |

**Areas**  

| Area Id  |                                     |
|----------|-------------------------------------|
| 0.0.0.20 | <input checked="" type="checkbox"/> |
| 0.0.0.0  | <input checked="" type="checkbox"/> |

Area Id  IP Address

Type  Ranges  Interface  Virtual Link

| Interface    | Enable                              | Passive                  | Link Type | Metric | Priority | Timing | Auth Profile |
|--------------|-------------------------------------|--------------------------|-----------|--------|----------|--------|--------------|
| ethernet1/15 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | broadcast |        |          |        | none         |

## 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:Opag-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
N/P:NSSA option, MC:multicast, 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:Opag-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
N/P:NSSA option, MC:multicast, 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      next-AS
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  
-----
```