Configuring IPSec VPN between overlapping networks

August 2010

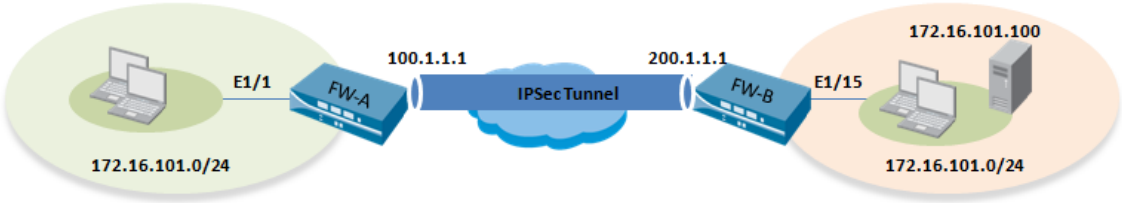
Palo Alto Networks
232 E. Java Dr.
Sunnyvale, CA 94089
408.738.7700
www.paloaltonetworks.com

Table of Contents

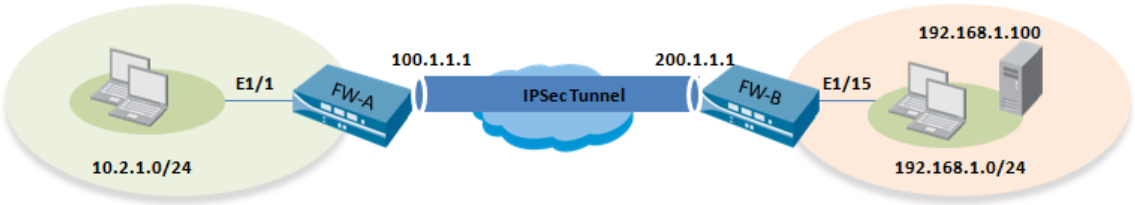
Overview

This document provides the configuration steps required to setup a route based IPSec tunnel between two overlapping networks using static routes and OSPF

Topology



The networks behind FW-A and FW-B have overlapping IP subnet. In this example, the clients behind FW-A is configured to access the server behind FW-B. NAT is used to translate network behind FW-A to 10.2.1.0/24 and network behind FW-B to 192.168.1.0/24. With address translation the network can be illustrated as shown below



Life of a packet

The table below shows the changes to IP address as it traverses the firewall

FW-A

Source IP address	Destination IP address	Comment
172.16.101.100	192.168.1.100	Original packet from the client accessing the server
10.2.1.1	192.168.1.100	Packet after source NAT
100.1.1.1	200.1.1.1	IPSec encapsulated packet as it leaves the FW-A.

FW-B

Source IP address	Destination IP address	Comment
100.1.1.1	200.1.1.1	IPSec encapsulated packet received by the FW-B
10.2.1.1	192.168.1.100	IP packet after encapsulating IPSec
10.2.1.1	172.16.101.100	IP packet after destination NAT.

Configuration on FW-A

Configure IPSec

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

IKE Gateway gw-to-siteB

Local IP Address ethernet1/2 100.1.1.1

Peer IP Address 200.1.1.1 ☐ Dynamic

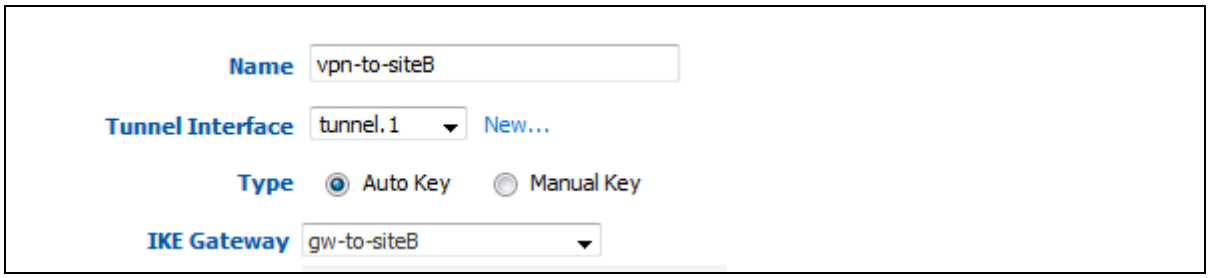
Select 'Dynamic' or enter a Peer IP Address

Pre-shared Key ••••••••••••••••••••••••

Confirm Pre-shared Key ••••••••••••••••••••••••

Show advanced Phase 1 options...

Network>IPSec tunnels



Security policy

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

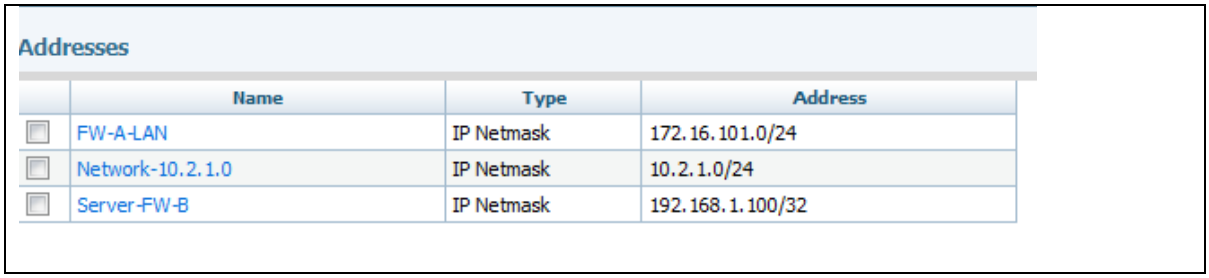
Source Zone	Destination Zone	Source IP	Destination IP	Application	Action
trust	vpn	172.16.101.0/24	192.168.1.0/24	any	allow

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

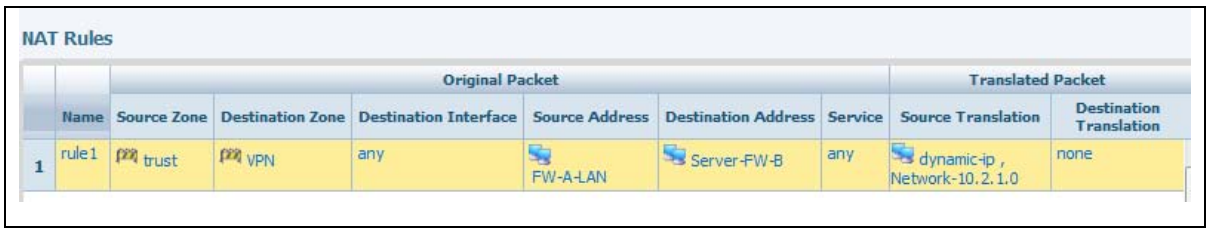
Source Zone	Destination Zone	Source IP	Destination IP	Application	Action
vpn	trust	192.168.1.0/24	172.16.101.0/24	any	allow

Source NAT configuration

The following address objects are created

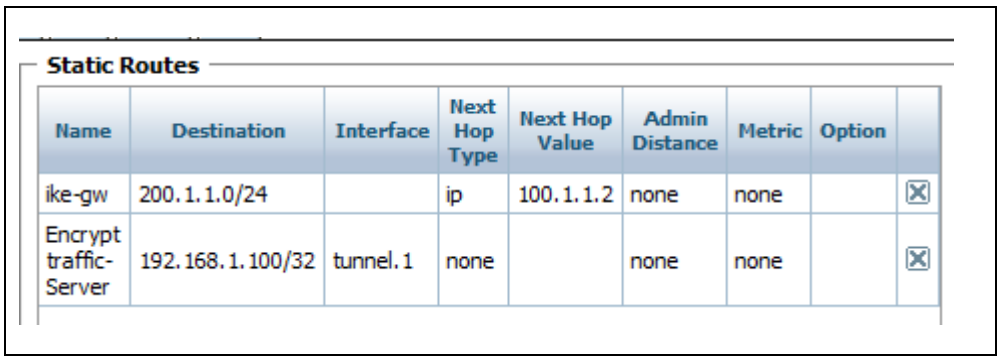


Configure a Source NAT rule as shown below



Routing configuration

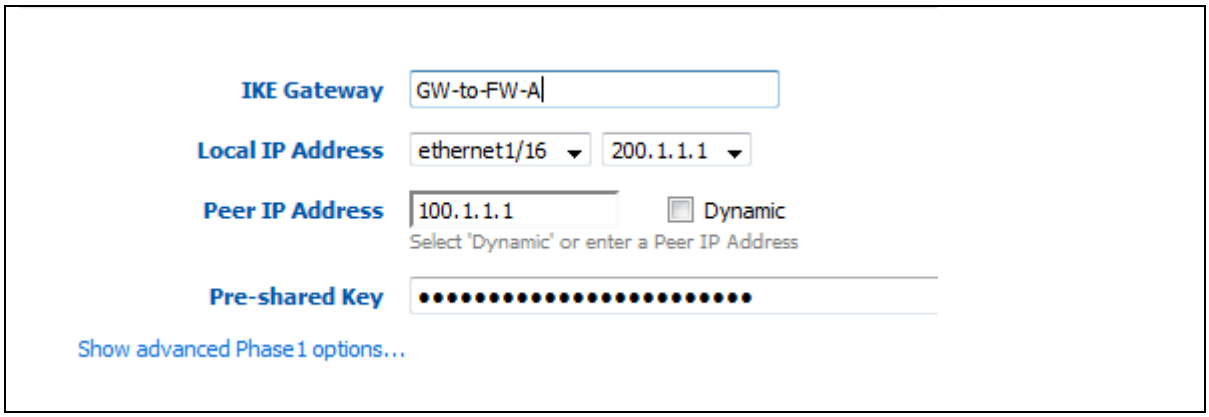
Static route to server address of 192.168.1.100/32 to the tunnel interface is required to encrypt all traffic to the server.



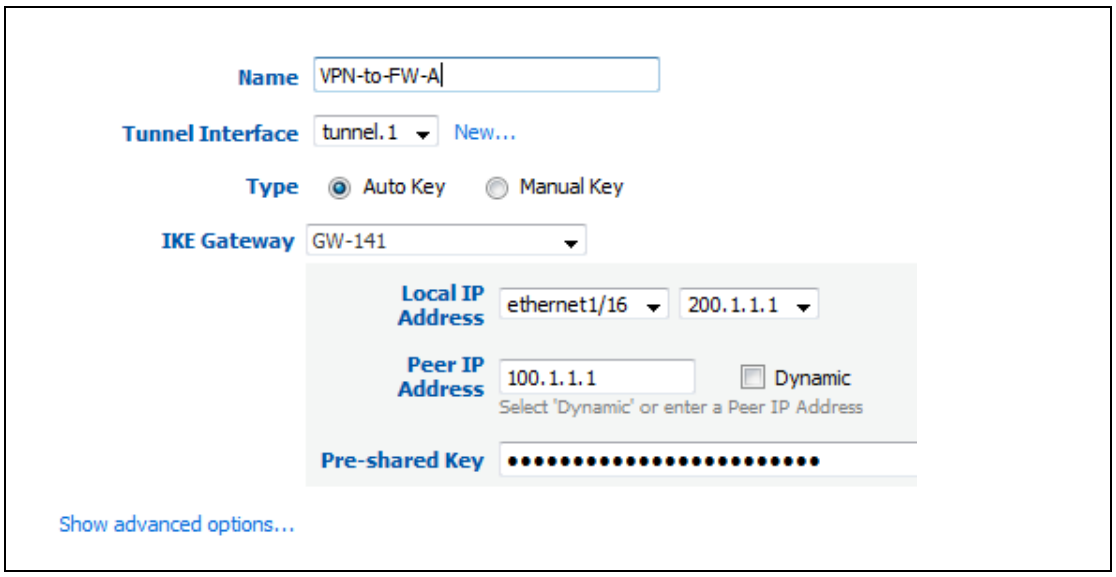
Configuration on FW-B

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 this example the following security policy is required

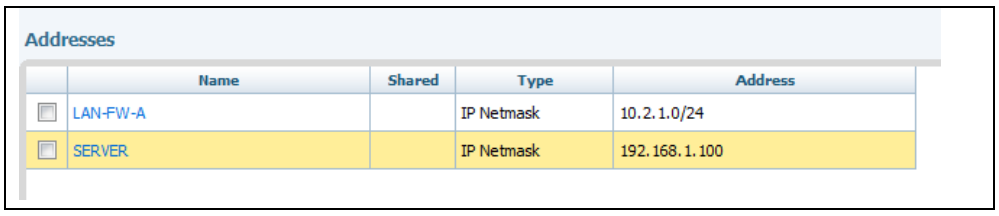
Source Zone	Destination Zone	Source IP	Destination IP	Application	Action
trust	vpn	172.16.101.0/24	10.2.1.0/24	any	allow

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	10.2.1.0/24	172.16.101.0/24	any	allow

NAT rule

The following address book entries are created to be used in the NAT rule



Configure a destination NAT rule as shown below

NAT Rules

		Original Packet					Translated Packet	
	Name	Source Zone	Destination Zone	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	VPN	trust-l3	LAN-FW-A	SERVER	any	none	172.16.101.100

Routing configuration

Static route to translated address 10.2.1.0/24 to the tunnel interface is required to encrypt all traffic from server.

Static Routes

Name	Destination	Interface	Next Hop Type	Next Hop Value	Metric	Option	
ike-gw	100.1.1.1/32	ethernet1/16	ip	200.1.1.2	none		
Encrypt traffic LAN-A	10.2.1.0/24	tunnel.1	none		none		

Using static NAT

Static NAT with bi-directional option can also be used in the scenario to enable communication between two sites. An example of NAT rule on the FW-A is shown below

NAT Rules

		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	rule1	trust	VPN	any	FW-A-LAN	LAN-B	any	static-ip , Network-10.2.1.0 , bidirectional: yes	none

Address objects used in the NAT rule is shown below

Addresses

	Name	Type	Address
	FW-A-LAN	IP Netmask	172.16.101.0/24
	LAN-B	IP Netmask	192.168.1.0/24
	Network-10.2.1.0	IP Netmask	10.2.1.0/24
	Server-FW-B	IP Netmask	192.168.1.100/32

Verification

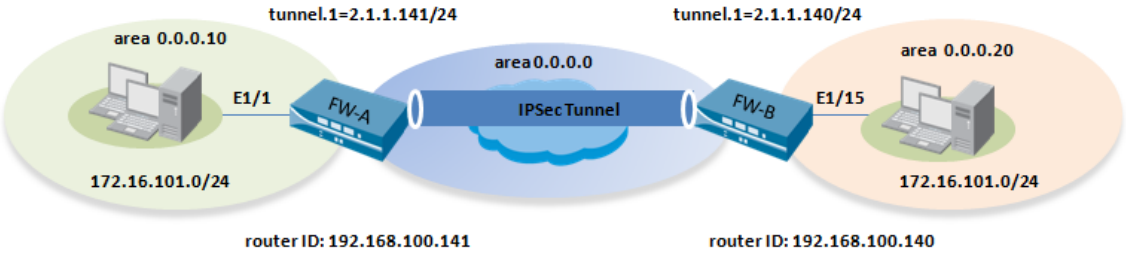
```
admin@FW-A> show vpn flow

--------------------------------------------------------------------------------
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
--------------------------------------------------------------------------------
```

```
admin@FW-A> show session all


flags: *:decrypted, N:NAT, S:src NAT, D:dst NAT, B:src and dst NAT
--------------------------------------------------------------------------------
ID/vsys   application     state   type flag   src[sport]/zone/proto (translated IP[port])
                                              dst[dport]/zone (translated IP[port])
--------------------------------------------------------------------------------

370/1     0               ACTIVE  TUNN        100.1.1.1[54992]/VPN/50 (100.1.1.1[46433])
                                              200.1.1.1[41340]/untrust (200.1.1.1[40824])
375/1     web-browsing    ACTIVE  FLOW  NS    172.16.101.100[1429]/trust/6 (10.2.1.0[1429])
                                              192.168.1.100[80]/VPN (192.168.1.100[80])

Display 1-2/2 sessions
```

Using OSPF

The NAT pools will have to be advertised by each of the firewalls to maintain reachability. One way to accomplish this is to create logical interfaces and assigning them IP address in the subnet of the NAT pool Tunnel interfaces are used in this example to advertise NAT pools.
Note: Loopback interfaces cannot be used to advertise a subnet used for NAT pool. The subnet mask used for loopback interfaces is always /32.

Topology



Configuration on FW-A

NAT pool: 10.2.1.0/24
Tunnel.200: 10.2.1.1/24"Inteface used to advertise the source NAT pool.
Tunnel.1 " Interface used to route IPSec traffic

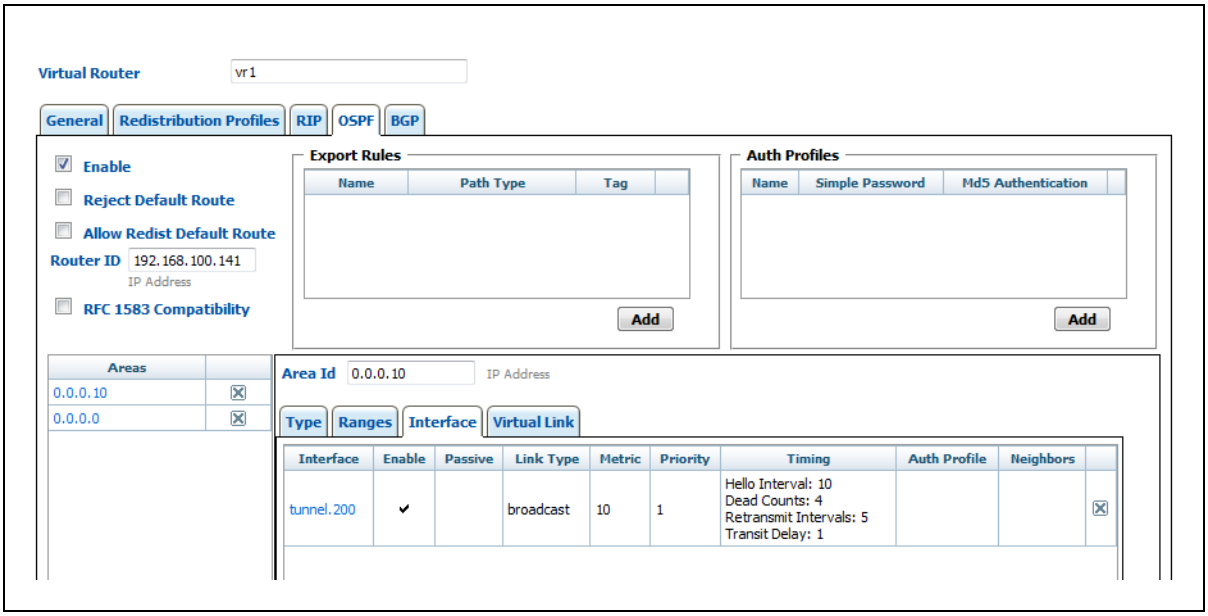
Zone configuration

Zones

	Name	Type	Interfaces / Virtual Systems
☐	L2trust	layer2	
☐	L2Untrust	layer2	
☐	trust	layer3	ethernet1/1 tunnel.200
☐	untrust	layer3	ethernet1/2
☐	VPN	layer3	tunnel.1
☐	vw-trust	virtual-wire	ethernet1/3 ethernet1/4

OSPF configuration

The tunnel.200 interface is assigned to area 10 and tunnel.1 is assigned to area 0



Configuration on FW-B

NAT pool: 10.2.1.0/24
Tunnel.100: 192.168.1.100/32"Inteface used to advertise the NAT pool.
Tunnel.1 "Interface used to route IPSec traffic

Verification

On the FW-A, you will notice that the route to the NAT address 192.168.1.100 is advertised via OSPF

```
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       1120128 tunnel.1
10.2.1.0/24             0.0.0.0                 10   Oi       1107284 tunnel.200
192.168.1.100/32        2.1.1.140               10 A Oo       683   tunnel.1
total routes shown: 3

admin@FW-A>
```

FW-B

Similarly on FW-B the route to the NAT address 10.2.1.0/24 is advertised via OSPF

```
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        1120100 tunnel.1
10.2.1.0/24              2.1.1.141            20     AOo        74532 tunnel.1
total routes shown: 2
```

Additional references

Configuring IPSec VPN
https://live.paloaltonetworks.com/docs/DOC-1163
Understanding NAT
https://live.paloaltonetworks.com/docs/DOC-1517