Configuring Site to site IPSec VPN in Layer 2 mode

August 2nd 2010

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

Table of Contents

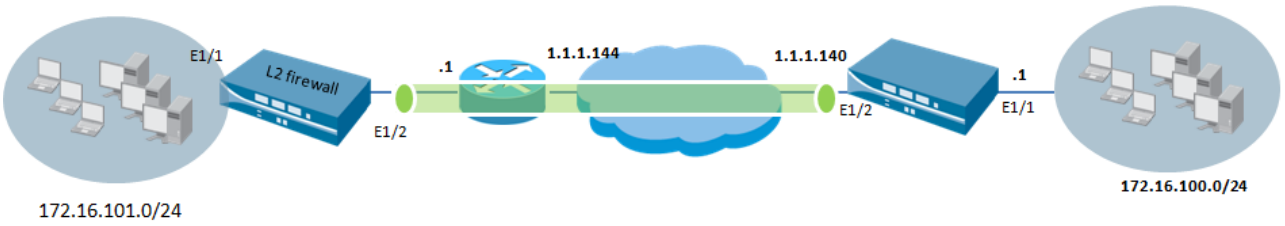
Overview

Palo Alto networks firewalls can deployed in the networks as Layer 2device offering all the security features. This configuration note walks through the details of configuring a site-to-site IPSec tunnel with the firewall deployed in layer 2 modes. This document covers the configuration on the Layer 2 firewall

Design consideration

With typical layer 2 deployments, the firewall is deployed in the exiting LAN usually assigned an IP address in the RFC 1918 space. Since these IP addresses are non routable in the public internet, you cannot use this interface for terminating IPSec connections originating from a site on public internet. One common way of addressing this issue is to configure a static NAT on the gateway router to the VLAN interface IP of the firewall that will be the IKE end point

Topology



In this example, there is only one VLAN configured on the firewall. All the layer 2 interfaces are assigned to the same VLAN. The tunnel is terminated on the VLAN interface.
The table below summarizes the networking configuration on the layer 2 firewall.

Interface	mode	VLAN	Zone	VR	IP address
Ethernet 1/1	Layer 2	test	L2trust	N/A	N/A
Ethernet 1/2	Layer 2	test	L2Untrust	N/A	N/A
VLAN.1	Layer 3	test	untrust	vr1	172.16.101.200/24
Tunnel.1	Layer 3	N/A	vpn	vr1	1.1.2.141/32

- The interfaces ethernet 1/1 and ethernet e1/2 are configured as part of VLAN object called test. VLAN.1 interface is used as the Layer 3 interface in the VLAN test to route traffic to the tunnel and also the IKE gateways end point
- All hosts must be configured with the VLAN interface as the default gateway in order to encrypt the traffic.. Any traffic to 172.16.100.0/24 will be sent to the VLAN1 interface.
- Route based tunnel is configured to route all traffic to the destination 172.16.100.0/24 to the VPN tunnel.

Configuration

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@PA-4050-141# show network interface ethernet ethernet1/1
ethernet1/1 {
  link-speed auto;
  link-duplex auto;
  link-state auto;
  layer2;
}
[edit]
admin@PA-4050-141# show network interface ethernet ethernet1/2
ethernet1/2 {
  link-speed auto;
  link-duplex auto;
  link-state auto;
  layer2;
}
```

```
admin@PA-4050-141# show network interface vlan
vlan {
  units {
    vlan.1 {
      mtu 1400;
       ip {
        172.16.101.200/24;
      }
    }
  }
 }
[edit]
```

```
admin@PA-4050-141# show network interface tunnel
tunnel {
  units {
    tunnel.1 {
      mtu 1400;
      ip {
        1.1.2.141;
```

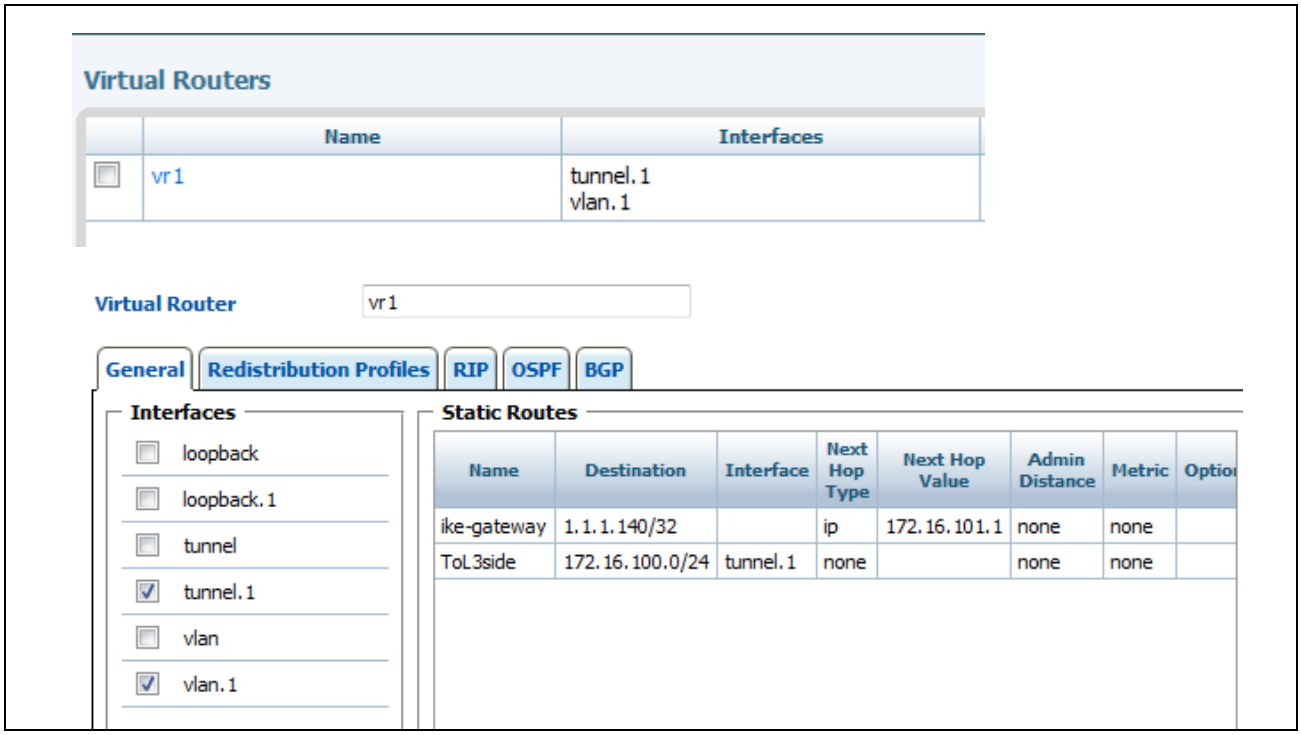
```
admin@PA-4050-141# show network vlan test
test {
  interface [ ethernet1/2 ethernet1/1];
  virtual-interface {
    interface vlan.1;
    l3-forwarding yes;
  }
}
```

Zone configuration

Zones

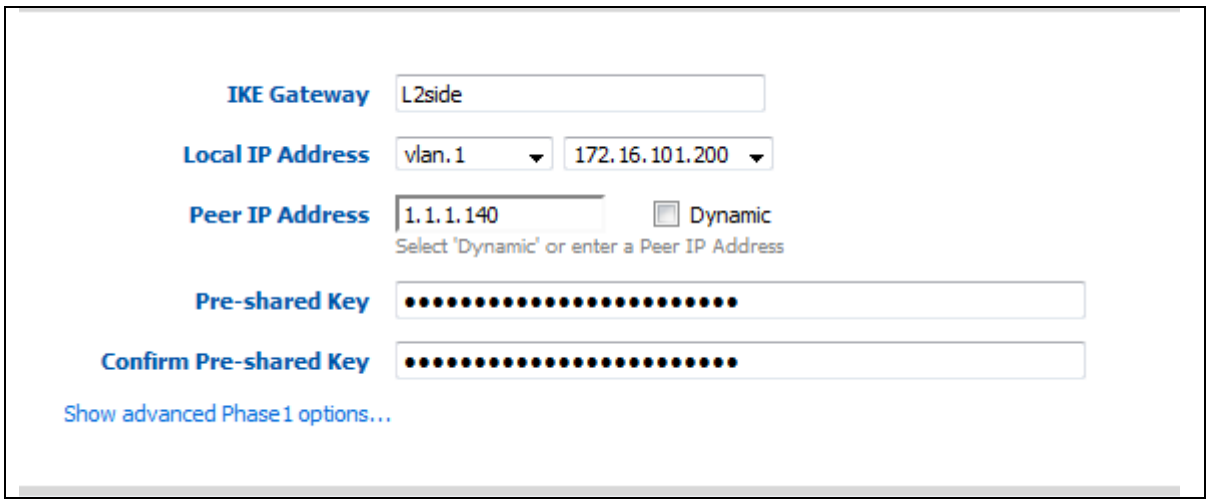
	Name	Type	Interfaces / Virtual Systems
☐	L2trust	layer2	ethernet1/1
☐	L2Untrust	layer2	ethernet1/2
☐	trust	layer3	
☐	untrust	layer3	vlan.1
☐	vlan	layer3	
☐	VPN	layer3	tunnel.1
☐	vw-trust	virtual-wire	ethernet1/3 ethernet1/4

Virtual router and routing configuration

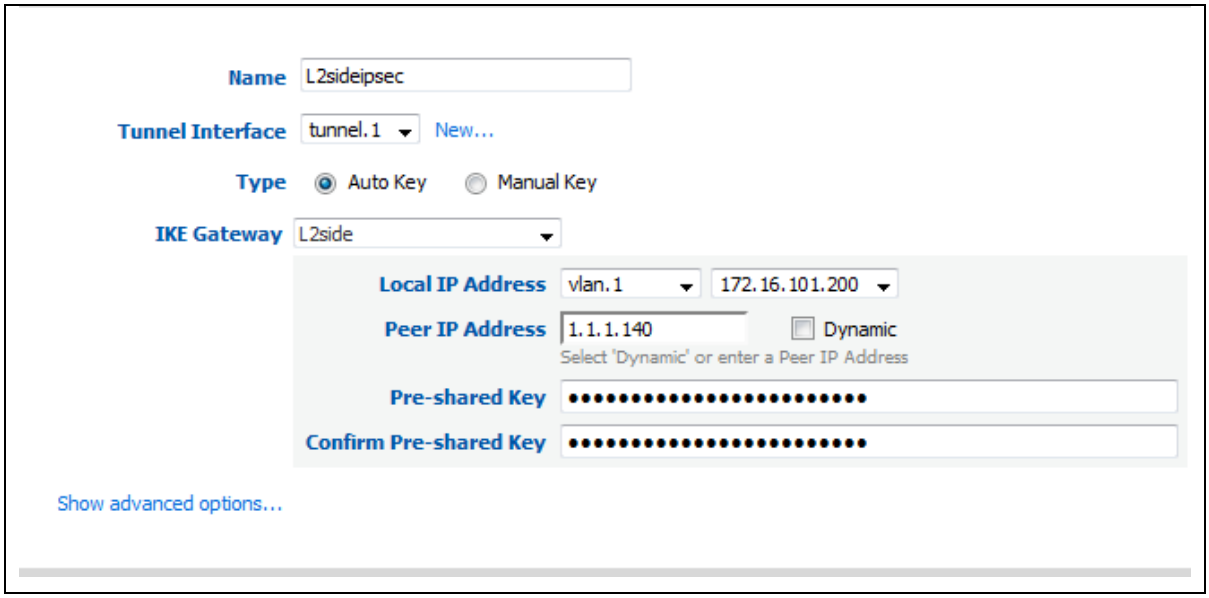


IKE and IPSec configuration

Network>network profiles> IKE gateways



Network>IPSec tunnels



Security policy

Security policies are required from the zone where VLAN1 interface resides 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
untrust	vpn	172.16.101.0/24	172.16.100.0/24	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	untrust	172.16.100.0/24	172.16.101.0/24	any	allow

Additional resources

For more details on configuring and monitoring IPSec refer to the following documents

https://live.paloaltonetworks.com/docs/DOC-1163

https://live.paloaltonetworks.com/docs/DOC-1236