Subject: IPsec packets from VEs sent to wrong interface
Posted by marcusb on Wed, 18 Jun 2008 08:42:44 GMT
View Forum Message <> Reply to Message

Hi,

I'm running OpenSWAN on the host node to provide tunnels to some VEs. The VEs are connected on veth devices that are bridged together to br0. The IPsec tunnel is correctly established, but response traffic from the VE is being sent out on br0, not the external interface eth0. Is there a workaround for this?

Details of the setup:

Server is OpenVZ 2.6.24 (compiled from git), Debian x86_64, OpenSWAN 2.4.12.

Host node interfaces:
eth0: public address 1.2.3.4 server.example.org
br0: bridge, internal address 172.16.1.1/24, only slave interface veth106.0
veth106.0: host end of veth.

VE interfaces:
eth0: veth interface, address 172.16.1.106

Now "ping 172.16.1.1" from the IPsec client (client.example.org with private address 172.16.2.2) works correctly, but "ping 172.16.1.106" shows this:
[host:~]# tcpdump -i br0
10:31:43.238582 IP 172.16.2.2 > 172.16.1.106: ICMP echo request, id 9274, seq 40, length 64
10:31:43.238617 IP server.example.org.4500 > client.example.org.4500: UDP-encap: ESP(spi=0xeee72df0,seq=0x35c), length 132
10:31:44.230477 IP 172.16.2.2 > 172.16.1.106: ICMP echo request, id 9274, seq 41, length 64
10:31:44.230509 IP server.example.org.4500 > client.example.org.4500: UDP-encap: ESP(spi=0xeee72df0,seq=0x35d), length 132

Here the packets destined for client.example.org are only seen on br0, not on the external interface. I have forwarding enabled on both br0 and eth0.

Cheers,

Marcus