Subject: Re: IPsec packets from VEs sent to wrong interface
Posted by Jerry Del Rio on Wed, 18 Jun 2008 21:04:51 GMT
View Forum Message <> Reply to Message

Marcus,

I would have a look at OpenVPN. OpenVPN works
as a client/server application when enabled. OpenVPN will
handle not just the tunnels but the routing for each
client as well as devices behind the clients that wish
to communicate with other clients or devices via the
VPN/tunnel. I haven't used the setup you are trying to do
but I think its feasible. If your VE's are not on the
same subnets then you should use VETH as you are doing,
otherwise a VENET device is fine if your ISP can get
you the block that you need.

Your initial hang up will be the tun device that needs
to be mapped to the VE's like this:

Allow your container to use the tun/tap device:

vzctl set 101 --devices c:10:200:rw --save
vzctl set 101 --capability net_admin:on --save

And create the character device file inside the container:

vzctl exec 101 mkdir -p /dev/net
vzctl exec 101 mknod /dev/net/tun c 10 200
vzctl exec 101 chmod 600 /dev/net/tun

***Anyone else correct me if I am wrong but I recall
somewhere that we can use the same host node tun device
for other VE's. This should enable other VE's that
are not the OpenVPN(server) to VPN as OpenVPN(clients).

Jerry Del Rio
Systems Engineer
949-331-4038 - Mobile
www.qunoc.com

Quoting Marcus Better <marcus@better.se>:

> 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
>
>

> --
> This message has been scanned for viruses and
> dangerous content by MailScanner, and is
> believed to be clean.
>

--
This message has been scanned for viruses and
dangerous content by MailScanner, and is
believed to be clean.