Subject: VPN inside VE, tunnel only specific traffic
Posted by tetra on Thu, 16 Apr 2009 19:30:17 GMT
View Forum Message <> Reply to Message

Hello,

I have a venet setup where the HN runs shorewall and controls the traffic going from and into the VEs. Each VE has one public IP.

Now I want to set up a VPN inside one of the VEs. I already got the VPN to work flawlessly but it redirects ALL traffic through the VPN which I do not want.

I thought about marking the packets inside the VE that should take the route through the VPN (based on the destination port) and then direct them to the appropriate routing table, but I don't know how I can accomplish this.

I experimented with iptables inside the VPN VE but it seems to conflict with shorewall somehow - at least the packets aren't marked at all.

What do you think is the best way of doing this? Is there maybe a way to set up the VPN on the HN and use it inside the VE? That way I could use shorewall for marking the packets.

I'm a little confused, sorry when I talk rubbish.

Edit: I think I got it:
echo 0 > /proc/sys/net/ipv4/conf/tun0/rp_filter
iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE
iptables -t mangle -A OUTPUT -p tcp --dport 80 -j MARK --set-mark 1
ip rule add fwmark 1 table vpn
ip route add default dev tun0 table vpn

I don't know if it's the optimal solution, but at least it works. (I tried marking in the POSTROUTING chain first, but I don't know why that doesn't work)