Subject: site-to-site VPN with OVZ
Posted by cdatgnp on Wed, 09 Jul 2014 23:16:41 GMT
View Forum Message <> Reply to Message

I am running into difficulty setting up a site-to-site VPN node on an OpenVZ instance. I'm cross-posting this here from my computerforum thread because I suspect some pecularity of OpenVZ may have something to do with this.

Goal
Establish communication between a remote PLC and our office. The PLC manufacturer recommends using a VPN to bridge the respective subnets.

Status
• D-Link VPN routers (DSR-150N) have been procured to use as the VPN hosts.
• The DSR routers have been configured with an IPsec policy.
• NAT routers at each end are administrated by other companies, with all external ports closed; it is desirable to be able to establish connection without opening ports to the Internet.
• Attempts to establish connection so far have failed despite attempting to use the NAT Traversal capability of the DSR routers; this could be because WAN ports are not open on either end.
• I am trying to set up a VPN node on a VPS to provide a node for both hosts to connect to.
• FQDNs are automatically updated to point to the respective external IP addresses of the remote site, our office, and the VPS node.
• We are now renting an OpenVZ container; this is desired due to cost, but maybe paying the incremental difference for a Xen instance would be worthwhile?
• strongSwan was installed to handle the IPsec configuration and to provide the charon daemon to automatically connect to the office and remote site hosts.
• strongSwan fails to connect; it reports that a NETKEY stack is absent and a KLIPS stack is absent. The OpenVZ wiki suggests that the kernel may not be recent enough to support IPsec from within a container.

Questions
Is there a better way to bridge the subnets in this situation?
Is this lack of a NETKEY/KLIPS (or other IPsec stack) the cause of my issue? -- There appears to be no TUN/TAP interface enabled for my VPS instance as well. Do I need this in addition to an IPsec stack?