【问题描述】

iptables在桥接模式下配置二层数据包转发

【解决方式】

iptables默认情况下关闭二层转发功能。可以在设置net.bridge.bridge-nf-call-iptables开启该功能，如果net.bridge.bridge-nf-call-iptables＝1，也就意味着二层的网桥在转发包时也会被iptables的FORWARD规则所过滤，这样就会出现L3层的iptables rules去过滤L2的帧的问题

【参考】

1. https://bugzilla.redhat.com/show_bug.cgi?id=512206
2. http://www.woitasen.com.ar/2011/09/confusion-using-iptables-nat-and-bridge/