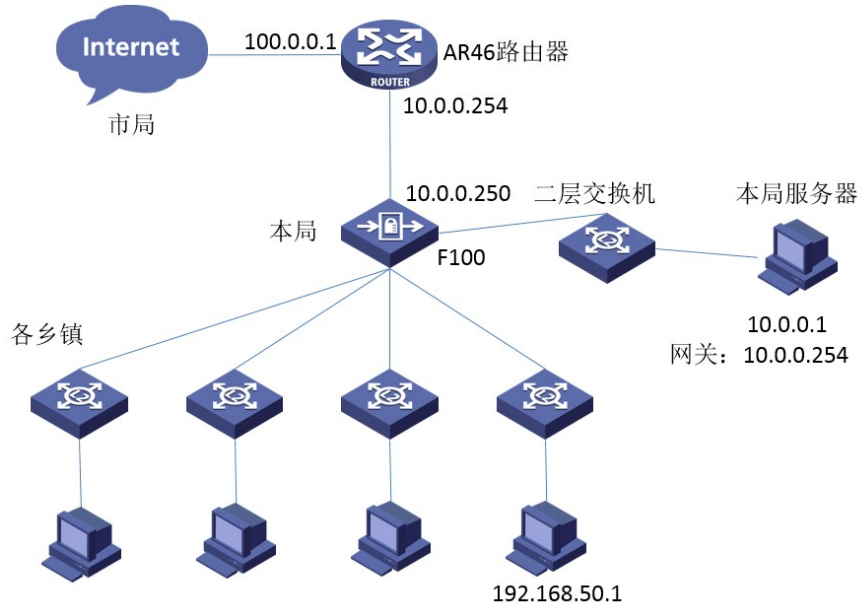
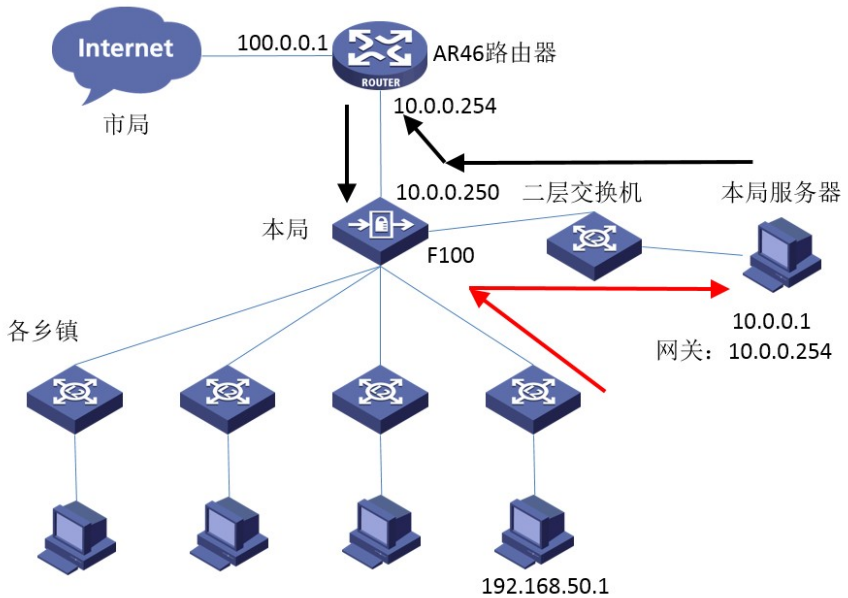
终端过F100-A-G2 ping不通服务器经验案例

菏新楼 2018-03-21 发表

本局的防火墙F100下连各个乡镇，各个乡镇出口为二层交换机，乡镇终端的网关在F100上。F100旁挂一台服务器，中间通过二层交换机互连。F100上连一台其他厂商的AR路由器，AR路由器作为服务器的网关并且通过外网连接市局。
现在各个乡镇的终端可以正常访问市局服务器，但是访问不了本局的服务器。



（1）在防火墙查看乡镇终端以及本局服务器的ARP学习正常，并且在防火墙上ping直连设备没有问题。
（2）防火墙域间策略为全放通。
（3）在本局的服务器上做ping测试，通过dis session table ipv4 verbose查看会话，发现从F100防火墙设备发出了5个ping包，回应为0个。初步怀疑是乡镇终端有没有正确配置网关，让其检查终端设置。确认乡镇终端配置无误后，乡镇终端依旧ping不通本局服务器，同时访问市局服务器正常。
（4）分析一下流量的经过，从乡镇的终端ping出来的包首先到达F100网关，F100通过直连路由传递给本局服务器。本局服务器的网关在AR路由器上，AR路由器与F100之间的互连地址和F100与本局服务器互连地址为同一网段。由于本局服务器和乡镇终端属于不同网段，本局服务器在回应的时候需要将报文先交给网关（AR路由器），然后AR路由器再查找路由表将报文送给防火墙。



这就导致了流量来回路径不一致，对于F100防火墙来说：会话状态机为严格模式。在非对称路径网络中，需要将会话状态机的模式配置为宽松模式，可以避免设备异常丢包。
在防火墙上将配置会话状态机为宽松模式：
[Sysname] session state-machine mode loose
当终端经过防火墙设备出现不通时，除了要注意域间策略外，还需要关注流量的走向。防火墙会话状

态机默认为严格模式，需要将其改为宽松模式，可以避免设备异常丢包或无法正常通信。
一般情况下，不建议改为宽松模式，可以规范现场组网以及IP地址分配。