同一个域名下的用户，比如同一个公司的员工，使用的企业邮箱后缀相同，这就是同域用户。

同域认证是邮件提供商服务器上的过滤规则，主要是用来拒收伪造地址的垃圾邮件，如果没有同域认证规则，您的邮箱会收到大量的伪造地址的垃圾邮件，即看到的发信人地址跟自己是一模一样的，或者域名是一样的。

同域认证规则规定了同一家邮件提供商内部投递的邮件必须通过服务商自己的 smtp服务器投递。如果同域下的邮件投递到了mx服务器上，服务器就会认为是伪造地址的垃圾邮件拒收， 因为mx服务器是用来接收外域邮件的。

以263企业邮箱为例：

可能有以下几种原因会导致发信人触犯263的同域认证规则：

263企业邮箱的用户所在的网络接入环境，限制了连接SMTP服务器的25端口，用户只能使用网络接入服务提供商提供的SMTP服务器发信，当给本域用户发信时，会产生退信；

某些自动转发也会导致触犯同域认证，比如ceshi@263.net 给 xxx@163.com 投递了邮件，xxx@163.com设置了自动转发，把邮件转发回 test@263.net的邮箱。 这样也可能会导致同域认证；

发信人在国外，客户端上填写的smtp服务器是正确的，但是可能当地的网络提供商设置了强制转发。当邮件数据到了他当地网络提供商的时候，被他们的服务器把邮件中转出来了；

用户使用一些特定的软件批量群发邮件，该软件直接具有解析收件方域名的MX记录和投递邮件的功能，不经过263的SMTP服务器发信，当收件方地址是本域名用户时，会产生退信；

用户使用blackberry（黑莓）手机，因黑莓手机无法指定发信服务器，用户发信时只要定义发件方地址，会直接利用黑莓手机自己的发信服务器来投递邮件，当给本域用户发信时，邮件被投递到MX服务器时，会触发同域认证规则，发件方会收到退信。

【处理方法】：

（1）、与用户了解放开同域认证的原因。

（2）、如果属于ISP限制用户连接SMTP服务器25端口的，可以指导用户使用SSL连接发信,

发件服务器：高级选项选中“√”SSL加密连接，端口：465

收件服务器：高级选项选中“√”SSL
加密连接，POP端口：995，IMAP端口：993

（3）、如果用户属于其他情况的，告知用户放开同域证后会造成本域内收到伪造地址的邮件，用户认可的，可以联系客服处理。

对于放开同域认证后，即使收件方的反垃圾级别是中级的情况，同域用户通过MX服务器投来的邮件，如果TAP网关判断具有垃圾邮件的特征，也会把邮件置入到不明文件夹中，不能保证一定进入收件箱。