防火墙做portal接口ldap后，用户流量统计还是显示地址或部分显示为用户
。

Portal认证 聂鹏 2021-10-19 发表

组网及说明

不涉及

问题描述

防火墙做portal后，用户正常认证，但是监控页面还是只有地址，没有显示用户。

过程分析

防火墙 用户流量统计显示为用户名，需要认证的用户能够识别为用户管理中的在线用户。
而用户管理中的在线用户识别有如下需求
1.能正常做portal认证。
2.用户管理中的用户身份识别包含现场认证的用户。
3.开启在线用户身份识别，并且portal认证用户能和用户身份识别中的用户对应。
由上可知，首先用户必须提前存在于防火墙中的用户身份识别，但是防火墙中，用户身份识别只有两种方式
1.手工建立本地用户
2.LDAP用户导入
而现在用户身份识别也有3中匹配方式。
keep-original：使用用户输入的用户名进行身份识别用户账户匹配。例如，用户的认证域为abc，用户输入的用户名为test@123，则使用用户名test@123进行身份识别用户账户匹配。
with-domain：使用用户的认证域进行身份识别用户账户匹配，即将采用“用户的纯用户名@认证域名”格式进行用户账户匹配。例如，用户的认证域为abc，用户输入的用户名为test@123，则使用用户名test@abc进行身份识别用户账户匹配。
without-domain：不对用户账户的域名进行匹配，即使用用户输入的纯用户名与设备上未加入任何身份识别域的身份识别用户账户进行匹配。例如，用户的认证域为abc，用户输入的用户名为test@123，则使用用户名test与未加入身份识别域的用户账户进行匹配。

综上所述，portal认证后监控页面能显示为用户是如下流程
portal认证——防火墙根据在线用户身份识别模式进行用户名调整——检查用户身份识别中是否有该用户——有则显示用户名，反之则反。

解决方法

根据上述流程。

1.首先检查设备portal及ldap认证是否正常。

2.检查手工配置用户或者导入策略是否正常。

3.检查是否开启在线用户识别，并且确认识别方式是否合理。如果使用withdomain 就是使用设备配置的ISP域名。如果使用withoutdomain，那就是只用用户名，并且匹配同步过来的用户时，也不能带域。keep-original就是按照用户portal认证登陆时使用的形式进行匹配。

这里有两个注意点，

1）模式不同，用户登录时是否使用域名的结果是不一样的，详情见上述案例。

2）用户导入策略同步过来的用户，如果也是带了域的，那么设备必须选择withdomain或者keep-original。