安全策略中放通用户不生效

SSL VPN AAA 域间策略/安全域 王树岭 2022-04-22 发表

问题描述

现场做sslvpn结合ldap认证，拨号和访问内网都正常

由于现场ldap服务器中没有对用户进行分组，想要在墙上用安全策略对用户进行访问权限限制。

某测试用户拨号成功之后，ping内网通，在策略调用该用户后，ping不通，被策略阻断。

过程分析

下面配置仅做举例：

sslvpn context中aaa domain名为ldap，在domain ldap中配置认证

实际上的用户域idendity domain 是h3c.com

测试用户为Alice，Bob

解决方法

首先需要开启用户身份识别功能（缺省关闭）：user-identity enable

另外，需要修改user-identity online-user-name-match，来配置在线用户身份识别的用户名匹配模式。分为以下三种：缺省为Keep-original

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。

①不修改，保持为Keep-original，拨号时使用用户名+用户域的形式，即Alice@h3c.com，Bob@h3c.com

②修改为with-domain，同时修改认证域名为h3c.com，与用户域一致，此时用Alice和Bob拨号

这两种方法可以匹配上身份识别用户，可以受到安全策略的控制。