V7防火墙做基于SSL VPN用户的安全策略

AAA 孔梦龙 2023-05-23 发表

组网及说明

V7防火墙做基于SSL VPN用户的安全策略

配置步骤

假设SSL VPN的用户不在本地，是在LDAP上，也就是说SSL VPN的用户认证是需要LDAP认证的；

先参考案例1：
基于用户的安全策略生效的过程（以某局点不能生效为例解释）
https://zhiliao.h3c.com/theme/details/188099
发现，要想被安全策略调用，实际上需要有在线用户，也就是说在线用户是安全策略调用的前提；
在本设备接入的在线网络接入用户。用户通过本地或远程服务器认证上线后，用户身份识别模块会在本地身份识别用户账户中查询该用户名和域名对应的表项，如果查询成功，则会生成一条在线身份识别用户表项。

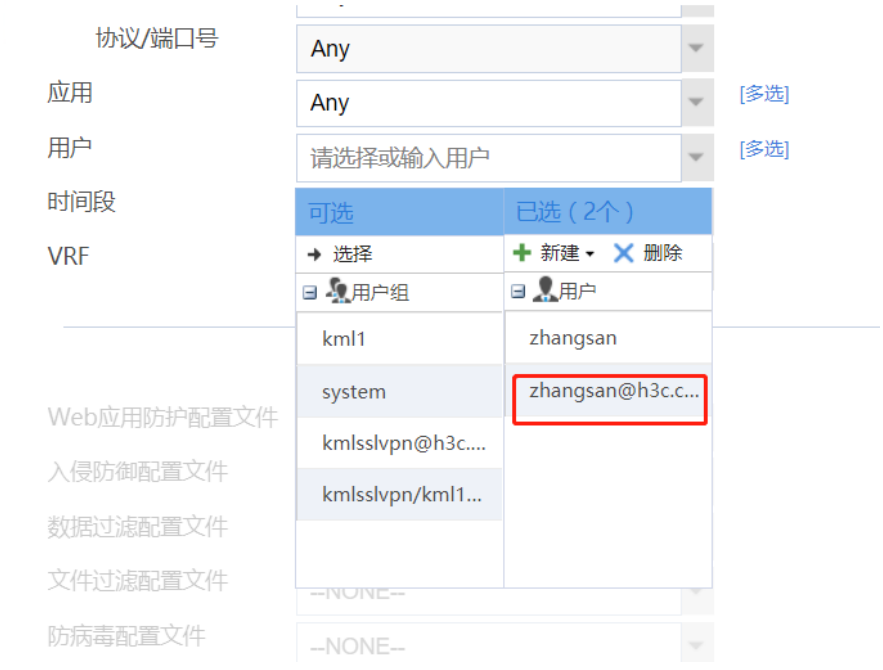
再参考案例2：
【完整版+解释】SSL VPN结合LDAP认证配置
https://zhiliao.h3c.com/Theme/details/165528
让SSL VPN用户上线；

因为：用户通过本地或远程服务器认证上线后，用户身份识别模块会在本地身份识别用户账户中查询该用户名和域名对应的表项，如果查询成功，则会生成一条在线身份识别用户表项。
所有身份识别模块需要有本地的用户数据，这个数据可以是本地创建的、LDAP上同步过来的、从CSV文件中导入，都行

最后参考案例3：
V7防火墙基于LDAP的用户导入案例
https://zhiliao.h3c.com/theme/details/218744
这就把用户同步过来了

最后在在线用户就可以看到这个用户了，然后安全策略中调用
rule 1 name test
action drop
user zhangsan domain h3c.com

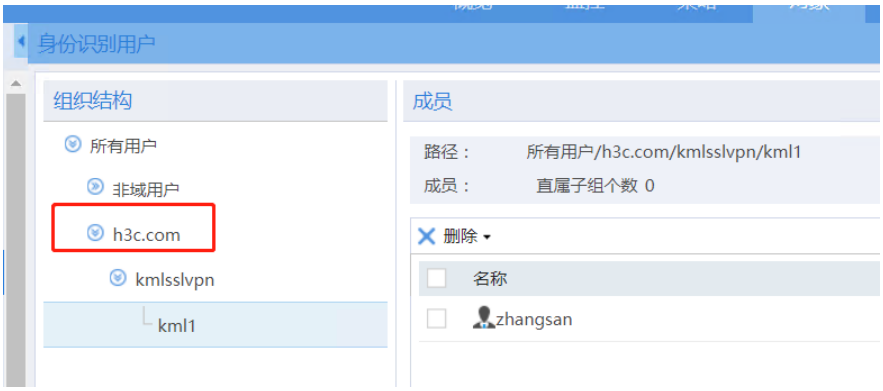
修改安全策略



配置关键点

LDAP上的用户zhangsan属于什么域，SSLVPN认证就需要怎么域，两者的名字保持一致：

例如：LDAP上zhangsan属于h3c.com这个域



ssl vpn认证的时候就需要同样的名字：

```
 service enable
#
sslvpn context sslvpn
 gateway gw
 ip-tunnel interface SSLVPN-AC1
 ip
  includ                    255.255.0
 policy-group pg1
  filter ip-tunnel acl 3001
  ip-tunnel access-route ip-route-list rtlist1
 aaa domain h3c.com
 service enable
#
```

同时查看在线用户的时候，需要开启身份识别和带域匹配