防火墙ssl vpn结合radius认证iNode报建立隧道失败

AAA SSL SSL VPN 刘诚 2021-12-24 发表

组网及说明

不涉及

问题描述

F1030防火墙结合radius服务器做ssl vpn iNode客户端报建立隧道失败

过程分析

debug ssl vpn有如下报错：

*Dec 23 00:03:17:148 2021 NW-FW1030 SSLVPNK/7/SSLVPN_ERROR: -COntext=1; IPAC: Failed to allocate an IP address. COntextID=0x2, OnlineID=0xc. //没有找到可用的地址，无法分配地址

*Dec 23 00:03:17:148 2021 NW-FW1030 SSLVPNK/7/SSLVPN_PACKET: -COntext=1; IPAC: Added data to packet. Data length=30, value=HTTP/1.1 551 Alloc IP Failed

.

*Dec 23 00:03:17:148 2021 NW-FW1030 SSLVPNK/7/SSLVPN_PACKET: -COntext=1; IPAC: Added data to packet. Data length=28, value=Server: SSLVPN-Gateway/7.0

.

*Dec 23 00:03:17:148 2021 NW-FW1030 SSLVPNK/7/SSLVPN_PACKET: -COntext=1; IPAC: Added data to packet. Data length=21, value=Content-Length: 0

核对配置：

domain域配置

```
# domain sslvpn authorization-attribute user-group group-test
 authentication sslvpn radius-scheme sslvpn
 authorization sslvpn radius-scheme sslvpn
 accounting sslvpn radius-scheme sslvpn
#
```

实例配置：

```
# sslvpn context testip gateway GW domain sslvpn
 ip-tunnel interface SSLVPN-AC1 ip-tunnel address-pool testip mask 255.255.255.0
 ip-route-list list-1
 include 172.66.10.7 255.255.255.255
 include 172.66.10.25 255.255.255.255
 include 172.66.10.128 255.255.255.255
 policy-group group-test filter ip-tunnel acl 3997
 ip-tunnel access-route ip-route-list list-1
 aaa domain sslvpn
 service enable
#
```

本地用户配置：

```
# local-user sslvpntest class network
 password cipher $c$3$fo+/rQJySk+FAwCTmRi/AzGADrL57+7A
 service-type sslvpn authorization-attribute user-role network-operator
 authorization-attribute sslvpn-policy-group group-test
#
```

问题就出在这个本地用户上，参考官网ssl vpn结合radius认证的典配发现，要在防火墙上创建一个用户组，来进行ssl vpn策略的授权，不是创建本地用户。可以理解为用户是radius服务器设置好的，通过用户组去获取服务器上的用户信息。

解决方法

删除本地用户，配置用户组：

11) 配置用户组，基于用户组对用户进行授权

配置用户组group1，授权给该用户组的策略组为pgroup。

[Device] **user-group group1**

[Device-ugroup-group1] **authorization-attribute sslvpn-policy-group pgroup**

[Device-ugroup-group1] **quit**