防火墙SSLVPN用户可以登录非授权策略组中的资源

SSL VPN　吴昊A　2024-01-11 发表

组网及说明

问题描述

使用wuhao用户登录sslvpn，用户授权策略组为11，即对应context 111中的资源

```
#
local-user wuhao class network
 password cipher $c$3$Hul4p6f7YCQRExHqGyyfUsWrbFcCvhM3yA==
 service-type sslvpn
 authorization-attribute user-role network-operator
 authorization-attribute sslvpn-policy-group 11
#
sslvpn context 111
 gateway 11 domain test
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool pool mask 255.255.255.0
 ip-tunnel web-resource auto-push
 login-message chinese 欢迎来到安全组
 login-message english Welcome to security-group
 logo file logo111.jpg
 webpage-customize system
 ip-route-list rlist
  include 20.0.0.0 255.255.255.0
 url-item 防火墙
  url https://77.78.79.1
  sso method basic
  sso basic custom-username-password enable
 url-item 知网
  url https://www.zhiwang.com
 url-list urllist
  heading web
  resources url-item 防火墙
  resources url-item 知网
 shortcut 1111
  execution url('http://1.1.1.1')
 policy-group 11
  ip-tunnel access-route ip-route-list rlist
  resources url-list urllist
 certificate-authentication enable
 authentication use any-one
 service enable
#
sslvpn context 222
 gateway 11 domain wuhao
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool pool mask 255.255.255.0
 ip-tunnel web-resource auto-push
 login-message chinese 欢迎来到安全组
 login-message english Welcome to security-group
 logo file logo111.jpg
 webpage-customize system
 ip-route-list rlist
  include 10.0.0.0 255.255.255.0
 url-item 防火墙
  url https://77.78.79.2
  sso method basic
  sso basic custom-username-password enable
```

url-item 知网
 url https://www.zhiwang.com
url-list urllist
 heading web
 resources url-item 防火墙
 resources url-item 知网
shortcut 1111
 execution url('http://1.1.1.1')
policy-group **22**
 ip-tunnel access-route ip-route-list rlist
 resources url-list urllist
default-policy-group 22
certificate-authentication enable
authentication use any-one
service enable
#

使用wuhao这个用户资源登录sslvpn context 222，inode中的域填写该实例中的域名wuhao，发现可以正常拨上去并且能访问222实例下的资源。

过程分析

正常情况下wuhao这个用户只授权了context 111下的策略授权组11，没有下发context 222下的策略授权组22，是不可能登录上context 222的。

#
local-user wuhao class network
 password cipher c3$Hul4p6f7YCQRExHqGyyfUsWrbFcCvhM3yA==
 service-type sslvpn
 authorization-attribute user-role network-operator
 authorization-attribute sslvpn-policy-group **11**
#

进一步排查实例下的配置，发现context 222 实例下配置了缺省的策略组 **default-policy-group 22，这个命令含义如下：**

default-policy-group命令用来指定缺省策略组。
undo default-policy-group命令用来恢复缺省情况。

【命令】

default-policy-group group-name
undo default-policy-group

【缺省情况】

未指定缺省策略组。

【视图】

SSL VPN访问实例视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-name：策略组名称，为1～31个字符的字符串，不区分大小写，支持输入中文字符。指定的策略组必须在设备上已经存在。

【使用指导】

一个SSL VPN访问实例下可以配置多个策略组。远端接入用户访问SSL VPN访问实例时，AAA服务器将授权给该用户的策略组信息下发给SSL VPN网关。该用户可以访问的资源由授权的策略组决定。如果AAA服务器没有为该用户进行授权，则用户可以访问的资源由缺省策略组决定。

【举例】

#指定名为pg1的策略组为缺省策略组。

```
<Sysname> system-view
[Sysname] sslvpn context ctx1
[Sysname-sslvpn-context-ctx1] policy-group pg1
[Sysname-sslvpn-context-ctx1-policy-group-pg1] quit
[Sysname-sslvpn-context-ctx1] default-policy-group pg1
```

【相关命令】

- display sslvpn context
- policy-group

即用户即使没有授权，也可以登录上对应实例下的缺省资源组。

解决方法

去掉这个命令后，可以实现不同的用户拨号访问对应的实例资源。