防火墙使用SSL VPN结合IMC认证，用户在IMC上，配置SSL VPN用户绑定IP地址案例

AAA SSL VPN 孔梦龙 2021-06-07 发表

组网及说明

不涉及

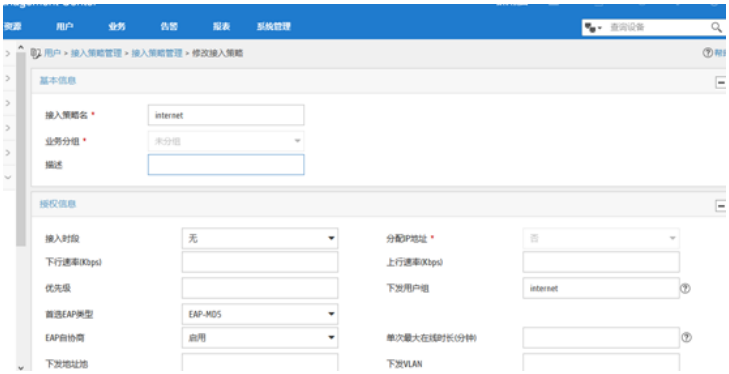
正常的FW上没有用户，用户在IMC上，PC使用inode拨号以后，FW转发用户信息到IMC上认证，并返回认证结果；

现场想使用SSL VPN用户绑定IP地址功能，即一个用户固定分配一个地址池中的一个IP。

配置步骤

FW ip绑定配置如下:

```
#
 user-identity enable
 user-identity static-user zhanxing bind ipv4 172.16.0.10
#
sslvpn ip address-pool internet 172.16.0.1 172.16.3.253
#
sslvpn context internet
 gateway internet domain internet
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool internet mask 255.255.252.0
 ip-route-list iplist
  include 0.0.0.0 0.0.0.0
  include 172.16.0.0 255.255.252.0
  include 172.16.201.0 255.255.255.252
  include 172.16.201.168 255.255.255.252
 policy-group internet
  filter ip-tunnel acl 3000
  filter web-access acl 3000
  filter tcp-access acl 3000
  ip-tunnel access-route ip-route-list iplist
 user zzzzz
  ip-tunnel bind address 172.16.0.10
 default-policy-group internet
 aaa domain internet
 service enable
#
user-group internet
 authorization-attribute sslvpn-policy-group internet
#
interface SSLVPN-AC1
 description intern
 ip address 172.16.3.254 255.255.252.0
#
```



用户还是在IMC上

FW上不用创建用户，但是要创建和IMC上一样的用户组

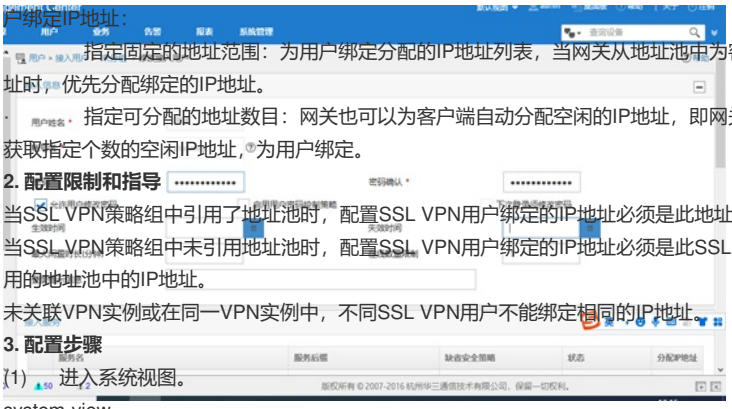
SSLVPN CONTEXT xxx 一定要创建用户

参考的配置手册为：

1.12.7 配置SSL VPN用户绑定IP地址

1. 功能简介

客户端使用IP接入方式访问SSL VPN网关时，网关需要为客户端分配IP地址。通过配置本功能，可以保证同一个用户多次访问该网关时能使用固定范围的IP地址。本功能提供以下两种方式为SSL VPN用户绑定IP地址：



指定固定的地址范围：为用户绑定分配的IP地址列表，当网关从地址池中为客户端分配IP地址时，优先分配绑定的IP地址。

指定可分配的地址数目：网关也可以为客户端自动分配空闲的IP地址，即网关会从地址池中获取指定个数的空闲IP地址，为用户绑定。

2. 配置限制和指导

当SSL VPN策略组中引用了地址池时，配置SSL VPN用户绑定的IP地址必须是此地址池中的IP地址。

当SSL VPN策略组中未引用地址池时，配置SSL VPN用户绑定的IP地址必须是此SSL VPN访问实例引用的地址池中的IP地址。

未关联VPN实例或在同一VPN实例中，不同SSL VPN用户不能绑定相同的IP地址。

3. 配置步骤

(1) 进入系统视图。

system-view

截图中的用户换成zzzzz，和FW上对应

(2) 进入SSL VPN访问实例视图。

sslvpn context context-name

(3) 创建SSL VPN用户，并进入SSL VPN用户视图。

user username

(4) 配置SSL VPN用户绑定的IP地址。

ip-tunnel bind address { ip-address-list | auto-allocate number }

缺省情况下，SSL VPN用户未绑定IP地址