V7设备（包含路由器，防火墙）做SSL VPN通过不同context实例使用多种认证方式做VPN接入认证案例

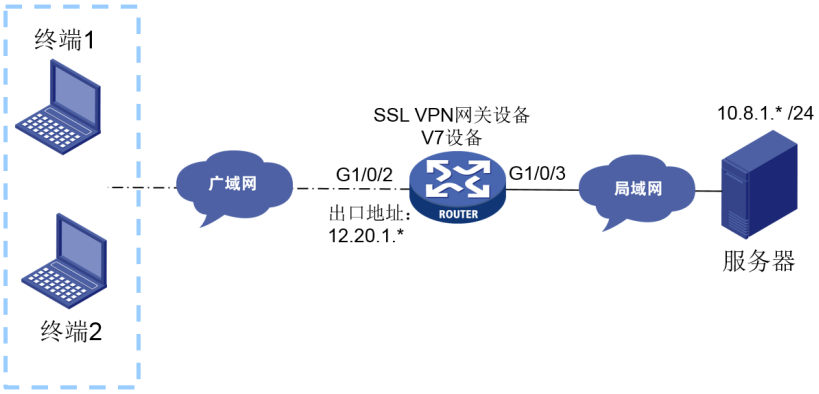
SSL VPN 徐猛 2021-03-26 发表

组网及说明

现场一台V7系列的路由器作为网络出口，同时设备上启用了SSL VPN用于远程接入用户的私网接入。同时在使用SSL VPN接入时，有如下需求：

（1）部分终端，图示中以终端1代替，要求在VPN接入时，使用SSL VPN网关设备上的本地账号进行登录认证，认证后终端获取VPN私网地址，并能够访问用户私网。

（2）其余部分终端，图示中以终端2代替，要求在VPN接入时，需要设备结合LDAP服务器进行账号登录认证，认证后终端获取VPN私网地址，并能够访问用户私网。



配置步骤

1.首先需要完成通用部分的配置：指定sslvpn下发的私网地址池，并指定sslvpn拨入时使用的gateway网关。

```
sslvpn ip address-pool sslvpnpool 172.16.0.2 172.16.255.254
#
sslvpn gateway gw
 ip address 12.20.1.*  port 4430
 service enable
#
```

2.完成LDAP相关的参数配置：

（1）LDAP服务器目录参数：

```
ldap server ldap1
 login-dn ljldap@guomaitech.com
 search-base-dn dc=guomaitech,dc=com
 ip 10.8.1.*
 login-password cipher $c$3$Qrt/4vaMtrY5vAPFgE2HTU+3GngyauPqmUGu+Q==
#
```

（2）LDAP认证方案参数：

```
ldap scheme fzlg
 authentication-server ldap1
 authorization-server ldap1
 attribute-map test
#
```

（2）LDAP属性映射参数：

```
ldap attribute-map test
 map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
#
```

（4）LDAP认证域

```
domain guomaitech
 authentication sslvpn ldap-scheme fzlg
 authorization sslvpn ldap-scheme fzlg
 accounting sslvpn none
#
```

3.指定local本地认证域参数：

```
domain local
 authentication sslvpn local
 authorization sslvpn local
 accounting sslvpn none
#
```

4.配置使用LDAP认证的SSL VPN认证context实例：

```
sslvpn context ctxip_ldap
 gateway gw domain guomaitech        //指定该SSL VPN实例的接入域为 guomaitech
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool sslvpnpool mask 255.255.0.0
 ip-tunnel keepalive 0
 ip-route-list rtlist
  include 172.20.0.0 255.255.255.0
  include 172.20.1.1 255.255.255.255
  include 172.20.1.2 255.255.255.255
  include 172.29.0.0 255.255.0.0
 policy-group resourcegrp
  filter ip-tunnel acl 3000          //ACl3000中进行允许访问的地址的放通
  ip-tunnel access-route force-all
  ip-tunnel access-route ip-route-list rtlist
  ip-tunnel address-pool sslvpnpool mask 255.255.0.0
 default-policy-group resourcegrp
```

aaa domain guomaitech **//指定该实例下认证使用的认证域为guomaitech**
timeout idle 60
log user-login enable
service enable

配置关键点
#
SSL vpn用户认证的时候，用户名位置不用添加@域名，域栏目中的内容为gateway后面关联的域字段。置使用local本地认证的SSL VPN认证context实例：
认证时会根据网关和域字段找到对应的context实例，使用实例中绑定的aaa domain做认证。

gnetwork-operator，授权

resourcegrp
perator

7.LDAP服务器上完成相应的管理和接入用户的创建。