SSLVPN + radius server authentication and authorization of the ACL for the clients configuration example

Security 蒋笑添 2021-07-09 Published

Network Topology

ISP --------- Firewall ---------- Radius server

Configuration Steps

The logical relationship of Radius attribute, user group and sslvpn policy is like following:
Radius Attribute 11 = user group name which can be got after user pass the auth on the Radius from the Radius server.
And sslvpn policy group is a attribute of user group. It should be defined on the device. Refer to:
Configuring user group attributes
authorization-attribute { acl acl-number | callback-number callback-number | idle-cut minutes | ip-pool ipv4-pool-name | ipv6-pool ipv6-pool-name | ipv6-prefix ipv6-prefix prefix-length | { primary-dns | secondary-dns } { ip ipv4-address | ipv6 ipv6-address } | session-timeout minutes | **sslvpn-policy-group group-name** | url url-string | vlan vlan-id | vpn-instance vpn-instance-name | work-directory directory-name } *
You can create sslvpn policy group which bind with exact acl policy. It should be defined on the device. Refer to:
Configuring an SSL VPN policy group for IP access
Finally, the relation map is Radius Attribute 11---- user group---- sslvpn policy group----acl. So the SSLVPN user can be get the corresponding ACL.

Configure Steps:
1. Configure the SSLVPN on the firewall.

```
#
sslvpn gateway gw
 ip address x.x.x.x port 4430
 service enable
#
interface SSLVPN-AC1
ip address 10.100.10.1 255.255.255.0
#
domain test.cn
 authentication sslvpn radius-scheme rscheme
 authorization sslvpn radius-scheme rscheme
 accounting sslvpn radius-scheme rsheme
#
sslvpn ip address-pool sslvpnpool 10.100.10.2 10.100.10.100
#
sslvpn context ctxip
 gateway gw
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool sslvpnpool mask 255.255.255.0
 ip-tunnel dns-server primary 10.30.10.11
 ip-tunnel dns-server secondary 10.30.10.12
 ip-tunnel log connection-close
 ip-tunnel log packet-drop
 ip-tunnel log address-alloc-release
 ip-route-list external
  include 192.168.0.0 255.255.255.0
 ip-route-list rtlist
  include 192.168.10.0 255.255.255.0
 policy-group external
  filter ip-tunnel acl 3013
  ip-tunnel access-route ip-route-list external
 policy-group resourcegrp
  filter ip-tunnel acl 3003
  ip-tunnel access-route ip-route-list rtlist
 default-policy-group resourcegrp
 log user-login enable
 log resource-access enable filtering brief
 service enable
#
```

2. create the user-group and bind the sslvpn policy group set in the sslvpn context.

#

user-group external

 authorization-attribute **sslvpn-policy-group external**

#

Key Configuration

3. Configure the attribute 11 on the Radius server.