SSLVPN本地账号绑定ip地址典型配置举例

SSL VPN 孙兆强 2023-12-10 发表

组网及说明

SSLVPN本地账号，客户想让账号绑定固定的ip，方便内网设备进行流量控制以及行为跟踪。

配置步骤

此处以缺省正式IP接入方式举例

(1)配置SSL VPN网关

配置SSL VPN网关gw的IP地址为1.1.1.2，端口号为4430。

<Device> system-view

[Device] sslvpn gateway gw

[Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 4430

[Device-sslvpn-gateway-gw] service enable

[Device-sslvpn-gateway-gw] quit

(2)创建SSL VPN客户端地址池

创建为SSL VPN客户端分配地址的地址池sslvpnpool，地址范围为10.1.1.1～10.1.1.10。

[Device] sslvpn ip address-pool sslvpnpool 10.1.1.1 10.1.1.10

(3)创建SSL VPN AC接口

创建SSL VPN AC接口1，配置该接口的IP地址为10.1.1.100/24。

[Device] interface sslvpn-ac 1

[Device-SSLVPN-AC1] ip address 10.1.1.100 24

[Device-SSLVPN-AC1] quit

(4)配置SSL VPN访问实例

配置SSL VPN访问实例ctxip，引用SSL VPN网关gw，指定域名为domainip。

[Device] sslvpn context ctxip

[Device-sslvpn-context-ctxip] gateway gw domain domainip

配置IP接入引用的SSL VPN AC接口1.

[Device-sslvpn-context-ctxip] ip-tunnel interface sslvpn-ac 1

创建路由表rtlist，并添加路由表项20.2.2.0/24。

[Device-sslvpn-context-ctxip] ip-route-list rtlist

[Device-sslvpn-context-ctxip-route-list-rtlist] include 20.2.2.0 24

[Device-sslvpn-context-ctxip-route-list-rtlist] quit

引用SSL VPN客户端地址池sslvpnpool。

[Device-sslvpn-context-ctxip] ip-tunnel address-pool sslvpnpool mask 24

创建SSL VPN策略组resourcegrp，引用路由列表rtlist，并同时配置对IP接入进行ACL过滤。

[Device-sslvpn-context-ctxip] policy-group resourcegrp

[Device-sslvpn-context-ctxip-policy-group-resourcegrp] ip-tunnel access-route ip-route-list rtlist

[Device-sslvpn-context-ctxip-policy-group-resourcegrp] filter ip-tunnel acl 3000

[Device-sslvpn-context-ctxip-policy-group-resourcegrp] quit

开启SSL VPN访问实例ctxip。

[Device-sslvpn-context-ctxip] service enable

[Device-sslvpn-context-ctxip] quit

创建ACL 3000，规则为允许源IP为10.1.1.0/24的报文访问目标IP网段20.2.2.0/24。

[Device] acl advanced 3000

[Device-acl-ipv4-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 20.2.2.0 0.0.0.255

[Device-acl-ipv4-adv-3000] quit

(5)配置SSL VPN用户

创建本地SSL VPN用户sslvpnuser，密码为123456，用户角色为network-operator，授权用户的SSL VPN策略组为resourcegrp。

[Device] local-user sslvpnuser class network

[Device-luser-network-sslvpnuser] password simple 123456

[Device-luser-network-sslvpnuser] service-type sslvpn

[Device-luser-network-sslvpnuser] access-limit 1 //限制用户同时在线数为1

[Device-luser-network-sslvpnuser] authorization-attribute sslvpn-policy-group resourcegrp

[Device-luser-network-sslvpnuser] authorization-attribute user-role network-operator

[Device-luser-network-sslvpnuser] quit

(6) SSL VPN访问实例ctxip中配置用户的ip地址

[F1030-NEW-sslvpn-context-ctxip]user sslvpnuser

[F1030-NEW-sslvpn-context-ctxip-user-sslvpnuser]ip-tunnel bind address 10.1.1.10

配置关键点

1、限制同一个用户同时在线数为1，否则超过的用户会从地址池中随机分配

2、如果用户绑定的地址已经分配出去，会强制之前用户下线。

3、分配的地址必须在地址池范围内

4、 authorization-attribute ip的方式对sslvpn用户不生效