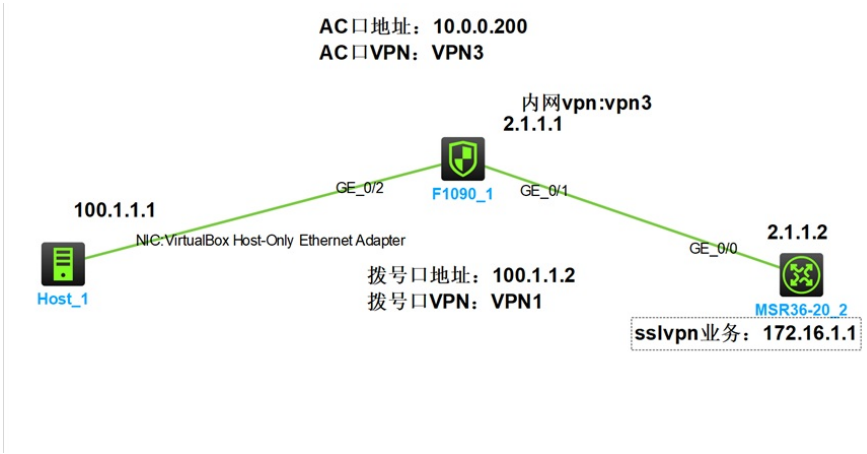
Comware V7 FW带VPN实例的SSLVPN典型配置

SSL VPN　孔德飞　2024-05-16 发表

组网及说明

组网如下：
拨号口带的VPN是VPN1，SSLVPN AC口与内网口带的VPN是VPN3
现在要实现的是在拨号口 AC口 内网口带有VPN实例的情况下，终端可以拨入SSLVPN，并且访问内网业务172.16.1.1



配置步骤

配置如下：
创建VPN实例
ip vpn-instance vpn1
ip vpn-instance vpn3

接口起IP并且绑定VPN实例
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpn3
 ip address 2.1.1.1 255.255.255.0

interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip binding vpn-instance vpn1
 ip address 100.1.1.2 255.255.255.0

创建SSLVPN地址池
sslvpn ip address-pool ippool 10.0.0.2 10.0.0.10

创建SSLVPN网关，要注意，SSLVPN网关所带有的VPN实例要与外网拨号口即100.1.1.2所在接口带有的VPN实例保持一致
sslvpn gateway gw
 vpn-instance vpn1
 ip address 100.1.1.2 port 2000
 service enable

创建SSLVPN实例，要注意，SSLVPN实例中所在的VPN实例，要与内网口即2.1.1.1所在的VPN实例一致
授权ACL口**一定不能绑定VPN实例**

acl advanced 3000
 rule 0 permit ip

```
sslvpn context 1
 vpn-instance vpn3
 gateway gw
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool ippool mask 255.255.255.0
 ip-route-list rtlist
  include 172.16.1.1 255.255.255.255
 policy-group pgroup
  filter ip-tunnel acl 3000
  ip-tunnel access-route ip-route-list rtlist
 service enable
```

接口加入安全域

```
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface SSLVPN-AC1
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
```

创建SSLVPN用户

```
local-user user1 class network
 password simple 123456
 service-type sslvpn
 authorization-attribute user-role network-operator
 authorization-attribute sslvpn-policy-group pgroup
```

放通安全策略

策略1放通的是拨号需要的安全策略，需要带着拨号口的VPN即VPN1

策略2放通的是拨号后VPN的业务，需要带着内网口的VPN即VPN3

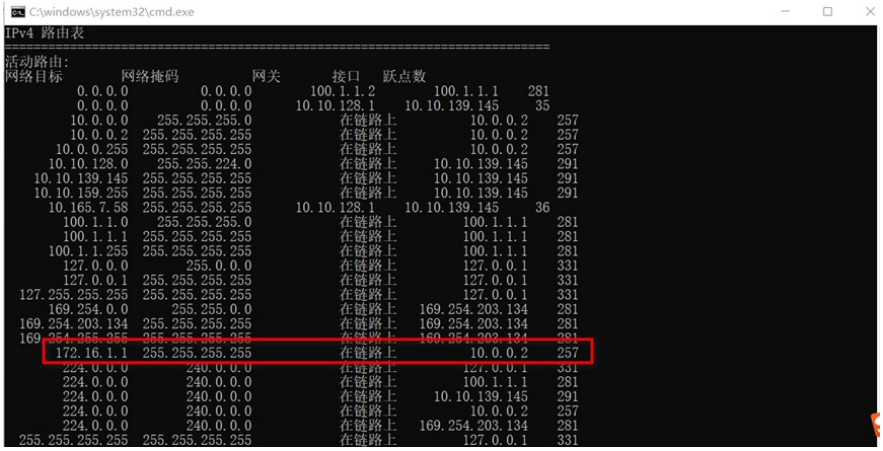
Sslvpn业务路由

```
ip route-static vpn-instance vpn3 172.16.1.0 24 2.1.1.2
```

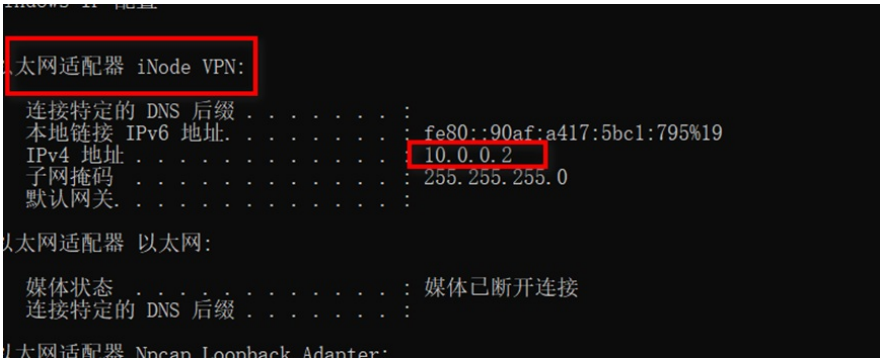
```
security-policy ip
 rule 1 name sslvpnbohao
  action pass
  vrf vpn1
 rule 2 name sslvpnyewu
  action pass
  vrf vpn3
```

终端可以拨入SSLVPN

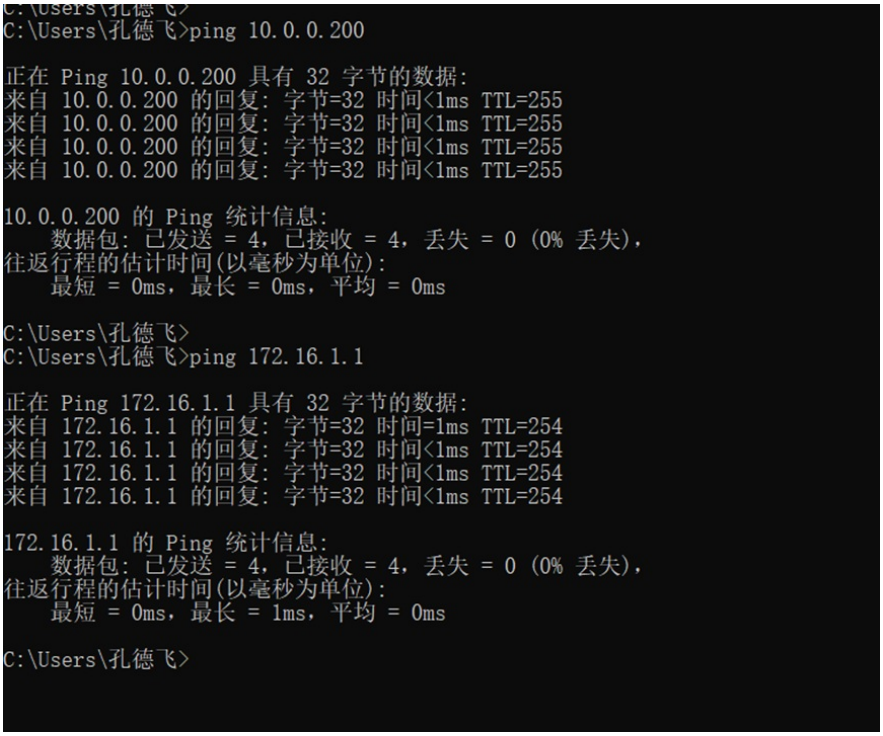
终端可以正常获取SSLVPN业务路由



终端可以正常获取SSLVPN地址池地址10.0.0.2



终端可以正常访问AC口地址以及SSLVPN业务地址



配置关键点

配置关键点:

1. 外网口拨号口带着什么VPN实例，SSLVPN网关就需要带着什么VPN实例
2. 内网口带着什么VPN实例，SSLVPN实例就需要带着什么VPN实例，为了SSLVPN拨入之后，终端可以正常访问AC口地址，AC口带的VPN实例必须与内网口保持一致
3. 安全策略需要放两个，第一个是拨号的策略，拨号口所在的安全域到local的安全策略，VRF是拨号口的VPN，第二个是AC口所在的安全域到内网口所在的安全策略，VRF是AC口所在的VPN
4. FW要写到SSLVPN业务的路由
5. SSLVPN实例中的授权ACL一定不能带有VPN实例