V7防火墙SSL VPN使用inode拨号不成功问题

SSL SSL VPN 马雷勇 2017-09-04 发表

在V7防火墙F1060上配置IP资源SSL VPN，在inode上进行拨号提示“查询SSL VPN网关参数失败，请检查网络配置或联系管理员。”

*Sep 4 19:23:48:553 2017 H3C SSLVPNK/7/SSLVPN_ERROR: -COntext=1; IPAC: No authority for IP access.
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_EVENT: -COntext=1; IPAC: The check result of the referenced address pool is 1.
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_EVENT: -COntext=1; IPAC: No uri-acl or no matched.
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_EVENT: -COntext=1; IPAC: The ACL check result is permit.
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_PACKET: -COntext=1; SSLVPN-AC1 input packet:
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_PACKET: -COntext=1; 0000 45 00 00 4e 4d ed 00 00 80 11 68 58 c0 a8 01 0a
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_PACKET: -COntext=1; 0010 c0 a8 01 ff 00 89 00 89 00 3a 9d 37 9b 68 01 10
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_PACKET: -COntext=1; 0020 00 01 00 00 00 00 00 00 20 46 48 46 41 45 42 45
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_PACKET: -COntext=1; 0030 45 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43
*Sep 4 19:24:12:378 2017 H3C SSLVPNK/7/SSLVPN_PACKET: -COntext=1; 0040 41 43 41 43 41 43 41 41 41 00 00 20 00 01

主要配置信息：

```
ip vpn-instance VPN
 route-distinguisher 200:1
#
interface LoopBack3
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet2/0/0
 port link-mode route
 ip binding vpn-instance VPN
 ip address 10.88.142.137 255.255.255.0
#
local-user h3c class network
 password cipher $c$3$84yUYr/NIRLDB17SQFRAcvh66V6IhQ==
 service-type sslvpn
 authorization-attribute user-role network-operator
 authorization-attribute sslvpn-policy-group pg
#
pki domain sslvpn
 public-key rsa general name sslvpn
 undo crl check enable
#
ssl server-policy ssl
```

pki-domain sslvpn
ciphersuite rsa_aes_128_cbc_sha
#
sslvpn gateway gw
ip address 10.88.142.137
ssl server-policy ssl
service enable
#
sslvpn context ctx
vpn-instance VPN
gateway gw
ip-tunnel interface SSLVPN-AC1
ip-tunnel address-pool ippool mask 255.255.255.0
ip-route-list list
include 3.3.3.3 255.255.255.255
include 192.168.100.0 255.255.255.0
policy-group pg
filter ip-tunnel acl 3001
ip-tunnel access-route ip-route-list list
service enable
#
对于报错，ping测试gateway地址是通的：
C:\Users\admin>ping 10.88.142.137
正在 Ping 10.88.142.137 具有 32 字节的数据:
来自 10.88.142.137 的回复: 字节=32 时间=1ms TTL=254
来自 10.88.142.137 的回复: 字节=32 时间=2ms TTL=254
来自 10.88.142.137 的回复: 字节=32 时间=2ms TTL=254
来自 10.88.142.137 的回复: 字节=32 时间=2ms TTL=254
查看证书情况也没问题：

```
[H3C]dis pki certificate domain sslvpn local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:07:08:a8:00:00:00:00:00:04
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=H3C-ICG
        Validity
            Not Before: Dec  1 06:16:50 2006 GMT
            Not After : Dec  1 06:12:01 2056 GMT
        Subject: C=CN, ST=Beijing, L=Beijing, O=H3C, OU=R&D, CN=SSL VPN
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b8:ab:a8:e3:c4:75:13:f8:f4:c7:16:a4:1f:ed:
```

```
[H3C]dis pki certificate domain sslvpn ca
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48:74:ec:e9:83:5c:86:8d:47:09:80:75:d2:4c:db:5e
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=H3C-ICG
        Validity
            Not Before: Dec  1 06:02:42 2006 GMT
            Not After : Dec  1 06:12:01 2056 GMT
        Subject: CN=H3C-ICG
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c1:e0:f5:4c:18:30:57:d3:d9:e0:ce:33:a0:6c:
                    62:61:4f:89:52:c0:91:e1:d2:9f:66:32:07:3a:3f:
```

配置也很标准；
查看外网接口配置加入了vpn实例，外网也能ping通接口地址说明路由都没问题，不然也不会通，还是检查ssl vpn配置问题，根据V7的ssl vpn典型配置看除了vpn实例外其他配置都类似，重点先查看不同配置侧，sslvpn context ctx实例也添加了vpn实例配置，查看手册了解到sslvpn context可添加vpn实例，另外sslvpn gateway下也可添加vpn实例，两个视图下配置vpn实例是实现不同的功能，
sslvpn context是vpn实例，用来匹配内网侧的服务资源，连接内部；
sslvpn gateway是ssl vpn网关，用来针对外网侧用户访问，连接外部，和V5有区别；
一方面讲，目前现象用户拨号不成功（提示网关参数错误）还未到内网服务侧

将sslvpn context视图下vpn实例移到sslvpn gateway视图下，拨号成功。

1、对于公网侧有vpn实例情况，需要将gateway网关也加入对应vpn实例。

2、sslvpn context是vpn实例，用来匹配内网侧的服务资源，连接内部，可针对内网划分实例进行对应配置；

sslvpn gateway是ssl vpn网关，用来针对外网侧用户访问，连接外部。