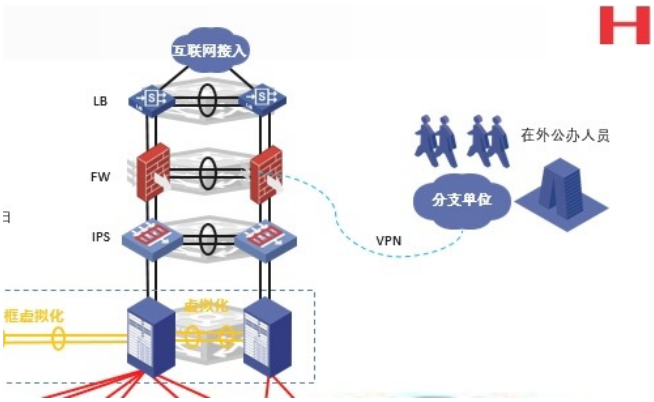
某局点终端SSL VPN 拨入后无法访问内网某些业务网段经验案例

SSL VPN　会话同步　刘资瑜　2018-12-05 发表

组网及说明

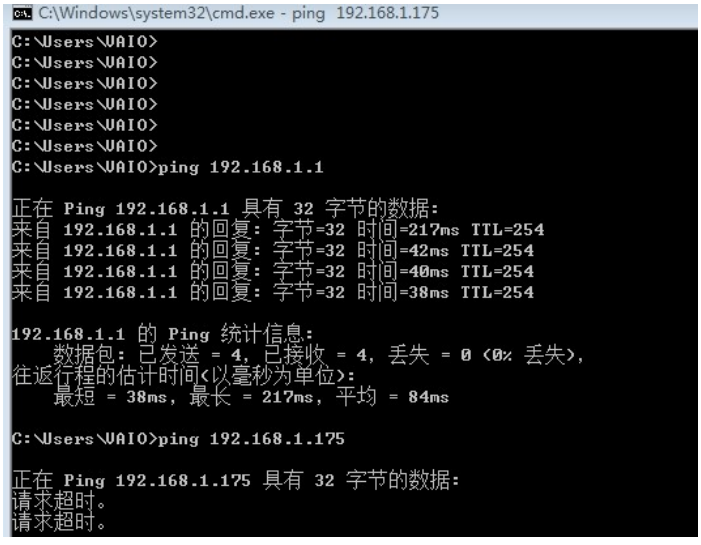


组网如上图所示，在防火墙1030堆叠后上做了SSL VPN，IPS做透传下联两台核心交换机做了堆叠。

问题描述

现场SSL VPN配置在防火墙上。外网接LB，LB上映射2000端口。

目前客户端拨入SSL VPN后(10.172.4.10)ping 核心交换机上地址192.168.1.1可以ping 通，但是ping不通下连业务地址192.168.1.175。



让现场在防火墙上带AC口（10.172.4.1）为源发现 ping 192.168.1.175可以通

```
******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<CWJT-New_F1030>
<CWJT-New_F1030>
<CWJT-New_F1030>
<CWJT-New_F1030>ping -a 10.172.4.1 192.168.1.175
Ping 192.168.1.175 (192.168.1.175) from 10.172.4.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.175: icmp_seq=0 ttl=63 time=1.074 ms
56 bytes from 192.168.1.175: icmp_seq=1 ttl=63 time=0.945 ms
56 bytes from 192.168.1.175: icmp_seq=2 ttl=63 time=0.770 ms
56 bytes from 192.168.1.175: icmp_seq=3 ttl=63 time=0.809 ms
56 bytes from 192.168.1.175: icmp_seq=4 ttl=63 time=0.789 ms

--- Ping statistics for 192.168.1.175 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.770/0.877/1.074/0.116 ms
```

过程分析

查看了终端路由表发现有到192.168.1.0/24网段的地址，且1030和核心上来回的路由都正常。因此让现场拨入SSL VPN后ping该业务段测试的同时在防火墙上查看会话。

```
  Slot 1:
  Initiator:
    Source IP/port: 10.172.4.10/1
    Destination IP/port: 192.168.1.175/2048
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: ICMP(1)
    Inbound interface: SSLVPN-AC100
    Source security zone: Untrust
  Responder:
    Source       IP/port: 192.168.1.175/1
    Destination IP/port: 10.172.4.10/0
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: ICMP(1)
    Inbound interface: Vlan-interface1000
    Source security zone: Trust
  State: ICMP_REQUEST
  Application: ICMP
  Start time: 2018-12-04 11:51:38  TTL: 35s
  Initiator->Responder:            12 packets         720 bytes
  Responder->Initiator:            0 packets          0 bytes

  Total sessions found: 1

Slot 2:
Initiator:
  Source  IP/port: 10.172.4.10/1
  Destination  IP/port: 192.168.1.175/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: SSLVPN-AC100
  Source security zone: Untrust
Responder:
  Source       IP/port: 192.168.1.175/1
  Destination IP/port: 10.172.4.10/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface1000
  Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Start time: 2018-12-04 11:51:38  TTL: 5s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            12 packets         720 bytes
```

发现来回路径不一致，因此，在1030上流量发生了跨框，查看1030配置发现，对外，1030将对外的接口加入了冗余口；对内，1030没有任何操作，相当于双主组网。

解决方法

通过查阅官网发现SSL VPN不支持双主组网，但是这种情况对外主备而对内双主，通过验证也是不支持的，同样会导致来回路径不一致问题。
通过让现场更改组网，将1030对内对外均做冗余口+冗余组方案，再在防火墙搜集会话发现业务正常，解决该问题。