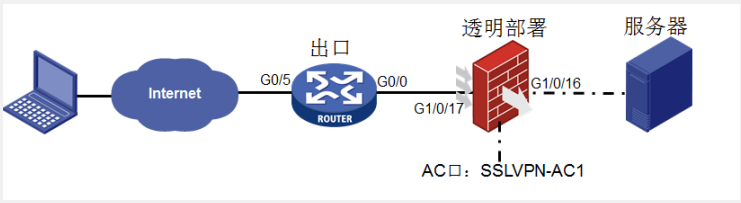
某局点F1030防火墙在内网透明模式部署，进行IP拨入方式的SSL VPN配置经验案例

SSL VPN　徐猛　2018-07-15 发表

组网及说明

现场拓扑图如下：网络出口使用我司的MSR3620，出口G0/5连接的电信运营商的公网专线。内网口G0/0连接在内网中透明部署的防火墙F1030，现场工程师描述，客户希望在该组网不变的情况下，使用外网的终端能够通过SSL VPN拨入防火墙，进而访问内部网络中的服务器。针对现场的这个需求，我们提出了建议，即：在透明部署的防火墙上，创建一个vlan的虚接口作为SSL VPN的网关，并让该网关地址和路由器能通（前提首先保证透明部署的情况下路由器到服务器能通）。并配置在路由器的公网出接口侧，将防火墙上的SSL VPN网关地址和端口通过nat server映射出去，并在防火墙上配置完成ip方式的SSL VPN后，公网的终端直接使用路由器的公网口地址和端口进行SSL VPN播入。**（为保护隐私信息，案例中涉及的公网地址均用*号进行部分隐匿）**



问题描述

指导现场根据上述思路进行配置完成后，现场使用Inode进行SSL VPN播入后，发现终端始终无法拨入成功，后续纠正现场的Inode拨入方式中存在问题后，能正常拨入并获取私网地址了，私网地址为10.10.1.1，但是仍然无法ping通和访问内网服务器，服务器地址为172.30.2.10。

过程分析

1. 对于最初现场工程师描述在终端使用INode进行拨入时，始终无法拨入成功的问题，我们首先检查下现场的相关配置：

内网防火墙侧：

```
#
interface Vlan-interface2501          //创建vlan 2501 的接口地址作为和路由器互联的SSL VPN网关地址
 ip address 172.30.250.4 255.255.255.248
#
interface SSLVPN-AC1          /创建SSL VPN的AC接口
 ip address 10.10.1.254 255.255.255.0
#
sslvpn ip address-pool SSLVPN_POOL 10.10.1.1 10.10.1.253
#
sslvpn gateway GW
 ip address 172.30.250.4 port 2000     /指定SSL VPN网关
 service enable
#
sslvpn context SSLVPN
 gateway GW
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool SSLVPN_POOL mask 255.255.255.0
 ip-route-list SSLVPN_ROUTE        /创建SSL VPN需要访问的服务器地址路由
  include 172.30.0.0 255.255.0.0
 policy-group SSLVPN_GROUP1
  filter ip-tunnel acl 3100
  ip-tunnel access-route ip-route-list SSLVPN_ROUTE  //策略组中添加向SSL VPN终端下发的SSL VPN路由
 log user-login enable
 service enable
#
```

acl advanced 3100　　//添加ssl vpn策略组中的acl规则
 rule 5 permit tcp source 10.10.1.0 0.0.0.255 destination 172.30.2.10 0 destination-port eq 3389
#
 ip route-static 0.0.0.0 0 172.30.250.1
 ip route-static 172.30.0.0 16 172.30.250.1　//去往服务器路由指向出口路由器内网口
 ip route-static vpn-instance mgt 0.0.0.0 0 172.30.254.254
#
interface GigabitEthernet1/0/16
 port link-mode bridge
 description to GJZY_ZYL_6F_WW_T1030_G1/0/17
 port access vlan 2501
#
interface GigabitEthernet1/0/17
 port link-mode bridge
 description to GJZY_ZYL_6F_WW_MSR3620_G0/0
 port access vlan 2501
#
出口路由器侧:
#
interface GigabitEthernet0/5
 port link-mode route
 description to 电信专线50M
 ip address *.105.64.254 255.255.255.0
 packet-filter 3999 inbound
 nat outbound 2000
 nat server protocol tcp global *.105.64.254 2000 inside 172.30.250.4 2000　　/对防火墙的SSL VP
N网关地址和端口进行nat server映射
#
interface GigabitEthernet0/0
 port link-mode route
 description to GJZY_ZYL_6F_WW_F1030_G1/0/17
 combo enable fiber
 ip address 172.30.250.1 255.255.255.248
#
 ip route-static 0.0.0.0 0 171.105.64.1 description to电信专线50M
 ip route-static 10.10.1.0 24 172.30.250.4　//去往终端私网地址，路由下一跳指向防火墙SSL VPN网
关接口地址（现场最初未配置该条目）
 ip route-static 172.30.0.0 16 172.30.250.6　　//去往内网服务器地址，路由下一跳指向服务器的网关
设备连接出口路由器侧的地址（图中未画出）。
#
　　检查了主要配置并未发现什么问题，后来指导现场先在web页面使用https:// *.105.64.254:2000/的
方式测试下看看能够弹出一个SSL VPN的web页面，现场描述可以，那说明我们的映射配置和SSL VP
N配置应该是生效了的，于是让现场工程师反馈INode拨号时使用的参数截图，发现现场参考官网的参
数，在INode的SSL VPN连接部分的域参数部分填写了domainip参数，但是现场配置中的SSL VPN网
关参数未指定所在域，让现场修改域参数后，INode拨入SSL VPN成功。

2.针对现场拨入终端成功获取私网地址10.10.0.1后，无法正常的ping通和访问内网服务器的问题，首先
让现场ping SSL VPN 的AC接口测试，发现能ping通AC接口，然后我们检查配置，服务器的私网路由
已经在vpn实例下发给了终端，且在终端的CMD控制台下通过route print命令查看终端路由表，是可以
查看到私网服务器的路由的。
 后来让现场在防火墙侧debug ip packet，debug信息如下：
*Jul 11 01:47:24:752 2018 GJZY_ZYL_6F_WW_F1030 IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 552, offset = 0, ttl = 64, protocol = 1
checksum = 48998, s = 10.10.1.1, d = 172.30.2.10
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface SSLVPN-AC1.　　//从ac接口收到报文
Payload: ICMP
 type = 8, code = 0, checksum = 0x4d3e.

*Jul 11 01:47:24:752 2018 GJZY_ZYL_6F_WW_F1030 IPFW/7/IPFW_PACKET: -COntext=1;
Sending, interface = Vlan-interface2501
version = 4, headlen = 20, tos = 0

pktlen = 60, pktid = 552, offset = 0, ttl = 63, protocol = 1
checksum = 49254, s = 10.10.1.1, d = 172.30.2.10
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Sending IP packet received from interface SSLVPN-AC1 at interface Vlan-interface2501. //从vlan2501接口发出
Payload: ICMP
  type = 8, code = 0, checksum = 0x4d3e.

可以从debug过程中看到，报文从防火墙的SSL VPN的AC接口收到后，已经正常的从网关接口interface vlan 2501发出去了，而报文下一跳就是出口路由器设备。说明不通问题并不是由于防火墙的原因。

于是我们继续在路由器上进行debug ip packet，观察报文在路由器上的路由转发过程是否异常，debug信息如下：

*Jul 11 18:05:20:721 2018 GJZY_ZYL_6F_WW_MSR3620 IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/0 //从互联的G0/0接口地址收到终端发给服务器的报文
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 198, offset = 0, ttl = 63, protocol = 1
checksum = 49608, s = 10.10.1.1, d = 172.30.2.10
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet0/0.
Payload: ICMP
  type = 8, code = 0, checksum = 0x4d56.

*Jul 11 18:05:20:721 2018 GJZY_ZYL_6F_WW_MSR3620 IPFW/7/IPFW_PACKET:
Sending, interface = GigabitEthernet0/0 //从互联的G0/0接口将终端发给服务器的报文发出去
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 198, offset = 0, ttl = 62, protocol = 1
checksum = 49864, s = 10.10.1.1, d = 172.30.2.10
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet0/0 at interface GigabitEthernet0/0.
Payload: ICMP
  type = 8, code = 0, checksum = 0x4d56.

*Jul 11 18:05:20:722 2018 GJZY_ZYL_6F_WW_MSR3620 IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/0 //从G0/0接口收到服务器给终端的回包
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 7705, offset = 0, ttl = 127, protocol = 1
checksum = 25717, s = 172.30.2.10, d = 10.10.1.1
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet0/0.
Payload: ICMP
  type = 0, code = 0, checksum = 0x5556.

*Jul 11 18:05:20:722 2018 GJZY_ZYL_6F_WW_MSR3620 IPFW/7/IPFW_PACKET:
Sending, interface = GigabitEthernet0/5 //从0/5将服务器给终端的回包路由转发出去。
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 7705, offset = 0, ttl = 126, protocol = 1
checksum = 25973, s = 172.30.2.10, d = 10.10.1.1
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Sending IP packet received from interface GigabitEthernet0/0 at interface GigabitEthernet0/5.
Payload: ICMP
  type = 0, code = 0, checksum = 0x5556.

从debug可以看出，服务器给终端的回包在路由器上未被正确的路由，本应从G0/0接口回包给防火墙的报文却从G0/5口转发走了，这是导致终端访问服务器不通的根因，后续让现场添加一条路由：

ip route-static 10.10.1.0 24 172.30.250.4 /在路由器上添加去往终端私网地址的下一跳指向防火墙的vlan interface 2501

添加该条目路由信息后，终端播入SSL VPN成功，且服务器就能够正常访问了。

解决方法

1. 现场防火墙部署在内网，并不是作为公网出口，所以这种场景下，要在出口设备上将SSL VPN网关地址和端口进行映射出去，又因为现场的防火墙使用的是透明模式部署在网络中，所以要使用vlan虚接

口和作为SSL VPN网关地址，并使用该接口地址和路由器对接，将终端的私网报文和路由器进行收发。整个流量传输过程大致为：外网终端使用使用自己获取的SSL VPN私网地址向私网服务器发送数据报文，然后在报文外层使用终端和对端的公网地址进行外层封装，后续报文会根据路由发送到出口路由器上，在出口路由器上匹配nat server后，路由器将报文发送给内网防火墙上的SSL VPN网关接口，在SSL VPN网关接口上匹配SSL VPN实例，对报文进行解封装为终端私网地址访问私网服务器地址，然后根据防火墙上的路由表，防火墙后续将报文由Vlan interface 2501接口发送给路由器，由于路由器和服务器可达的，后续再由路由器查找路由表，对报文进行路由，最终报文发送到服务器。服务器回包过程类似，回包过程需要注意，在路由器上需要有回包给终端私网地址段的路由，并在路由信息中下一跳指向防火墙的SSL VPN网关接口，详细过程在此不再赘述。

2. 在这种场景下，使用INode进行SSL VPN拨入时，Inode上网关地址要填写映射的公网地址和端口，同时要填写用户实例中对应的域名

3. 由于终端使用的是SSL VPN中分配的私网地址进行私网服务器的访问，所以私网中的网络设备上要添加去往该私网段的回程路由，保证报文能够回到防火墙的网关口上。

4. 该局点客户后续又增加了需求，需要内网终端也进行SSL VPN的拨入后才能访问内网服务器，在这种组网情况下，满足这种需求就会变的容易很多，

只需要在出口路由器的内网口添加公网口上的nat server配置，同时添加nat outbound配置，后续现场操作后需求满足。