Cisco AnyConnect VPN Client 无法访问用户内网

目录

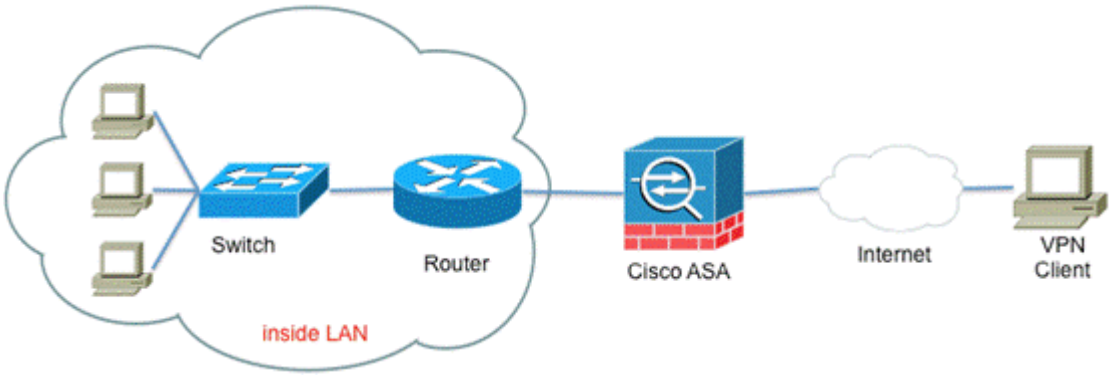
技术领域

AnyCOnnect, VPN, ASA

问题描述

用户通过Cisco AnyConnect VPN Client建立SSL VPN连接到 ASA，发现无法访问ASA inside端的内网网络

拓扑环境



故障排查步骤

以防火墙为节点，整个网络被划分为两个部分，内部网络（inside）和外部网络（outside），所以排查点就有三个：防火墙外部网络，防火墙自身，防火墙内部网络。

1. 排查防火墙外部网络：即VPN客户端到ASA outside接口部分，主要有以下两点需要排查：VPN客户端公网地址与防火墙outside接口之间连接性是否正常：通过公网地址之间互ping，可以排查。VPN客户端是否已经连接上ASA，并正常获取防火墙端地址池的地址,如下图所示:

2. 如果防火墙外部网络检查没有问题，但是仍然发现VPN客户端没法访问客户内网资源，就需要进一步排查问题究竟处在防火墙本身还是客户内网，常规手段我们会进行抓包，以确定问题究竟出在哪个环节，但今天要介绍的是一个更为快捷的确定故障点的方法：开启防火墙inside接口的management access功能。Management access 本身的设计初衷是当你有一个接口用于VPN连接的时候，你希望通过另外一个接口来登陆你的ASA，你可以通过把这个接口标示为management-access接口。举个例子来说，你是从ASA outside接口来进入ASA的，当你打开在inside 接口打开management-access功能的时候，你就可以从外网通过ASDM，SSH，telnet或者SNMP连接到ASA的inside接口地址，也可以从外口ping通ASA的inside端口地址。但需要注意的是，management-access 接口只能定义一个。Management-access功能可以通过如下命令打开，下例中我们在inside接口打

ASA1

```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)# management
ciscoasa(config)# management-access ?

configure mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/1
  outside  Name of interface GigabitEthernet0/0
ciscoasa(config)# management-access inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

：虽然这不是一个本身设计用来排错的命令，但在实际应用过程中，我们发现对于排查无法访问内网的问题，该命令能够十分快捷的排查故障点具体是在防火墙本身，还是在客户内网。

3. 开启防火墙inside接口的management access功能之后，从VPN客户端ping 防火墙inside接口的IP地址：如果ping成功，表明防火墙本身配置没有问题，应检查客户内网环境，常见问题是客户内网路由设计有问题，导致没有回程路由，或者内网的连通性都存在问题。我们可以进一步通过抓包来验证，如下例，我们通过在防火墙上配置抓包命令，在防火墙inside接口抓到如下包：

```
ciscoasa# show capture cap
 5 packets captured
 1: 23:22:16.604399 10.1.1.254 > 10.1.1.253: icmp: echo request
 2: 23:22:16.609129 10.1.1.254 > 10.1.1.253: icmp: echo request
 3: 23:22:16.612257 10.1.1.254 > 10.1.1.253: icmp: echo request
 4: 23:22:16.616072 10.1.1.254 > 10.1.1.253: icmp: echo request
 5: 23:22:16.620985 10.1.1.254  > 10.1.1.253: icmp: echo request
```

从上述抓包可以看出，icmp request包已经从inside接口送出，但是未收到回应，佐证了我们之前的判断，是客户内网存在问题。如果ping未成功，则我们首先要排查防火墙自身的问题，对比Anyconnect VPN相关配置文档，检查自己的配置，如果检查配置仍然未能排查出错误，请联系思科TAC部门寻求帮助。

4. 如果之前步骤都排查完毕，我们应该已经可以正常访问客户内网，可以通过抓包来进一步验证：

```
ciscoasa# show  capture cap-out
10 packets  captured
 1: 23:22:16.604399 10.1.1.254 >  10.1.1.253: icmp: echo request
 2: 23:22:16.608916 10.1.1.253 >  10.1.1.254: icmp: echo reply
 3: 23:22:16.609129 10.1.1.254 >  10.1.1.253: icmp: echo request
 4: 23:22:16.612044 10.1.1.253 >  10.1.1.254: icmp: echo reply
 5: 23:22:16.612257 10.1.1.254 >  10.1.1.253: icmp: echo request
 6: 23:22:16.615843 10.1.1.253 >  10.1.1.254: icmp: echo reply
 7: 23:22:16.616072 10.1.1.254 >  10.1.1.253: icmp: echo request
 8: 23:22:16.620771 10.1.1.253 >  10.1.1.254: icmp: echo reply
 9: 23:22:16.620985 10.1.1.254 >  10.1.1.253: icmp: echo request
10: 23:22:16.623869 10.1.1.253 >  10.1.1.254: icmp: echo reply
```

可见去包和回包都已经正常。

总结

1. 遇见AnyConnect VPN 无法访问内网的问题，包括其他AnyConnect VPN连接的问题，首先要排查出故障发生的部位是在防火墙内部网络，防火墙外部网络，还是在防火墙本身，这样能缩小我们排查范围，更快找到故障点。
2. 通过在防火墙inside接口打开Management-access命令可以帮助我们很快区分问题是在防火墙内部网络还是防火墙本身，比起传统的抓包和相应的debug工具等，能更快的定位故障点。
3. 抓包是我们在防火墙排错过程中最有效的工具，但有时候并不一定是最快捷的，要灵活使用。