某局点防火墙SSLVPN结合LDAP认证inode报错：和网关通信超时

SSL VPN SSL AAA iNode **曾招维** 2021-09-29 发表

组网及说明

组网：**测试PC**(XXX.104.145.154)—公网—(XXX .112.234.134:9527) **F1000-AI-60**(XXX .100.58.253)---(XXX .100.100.52)**LDAP服务器**

问题描述

现场开局，SSLVPN本地密码认证可以连接，但如果切换到结合LDAP密码认证就报VPN通信超时和系统内部错误问题。

Inode拨号方式及报错如图：

直接用web方式登录报错如下：

过程分析

1、参考典型配置检查防火墙SSLVPN结合LDAP认证基本配置：

相关配置可参考官网和知了案例https://zhiliao.h3c.com/Theme/details/165528

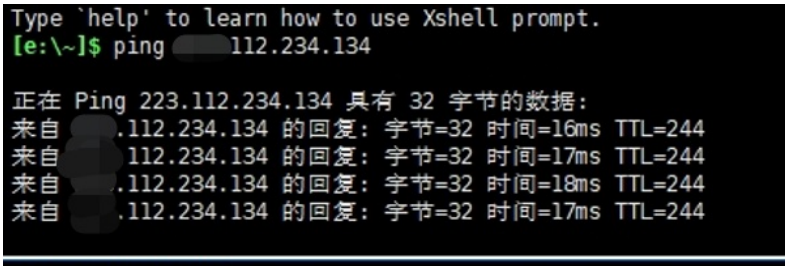
A、安全策略：外网口属于Untrust，内网口是trust，连接LDAP是LDAP域，AC口在AC域；SSLVPN拨号需要放通Untrust到Local，认证需要放通local到LDAP，访问内网资源需要放通AC域到trust。【按现场的实际情况，开局建议先使用全通策略，避免策略阻断】

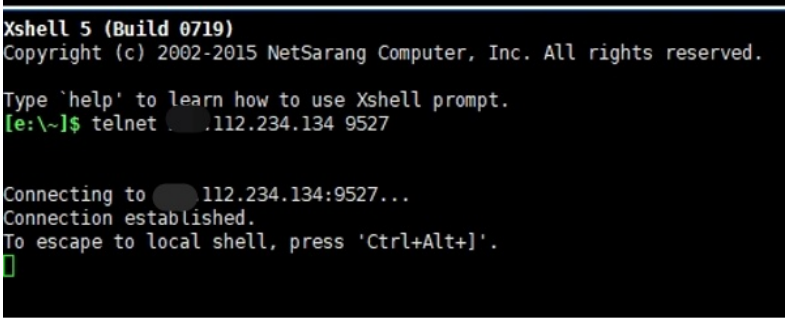
B、LDAP相关配置：确保LDAP侧配置和设备侧一致，创建LDAP相关的domain域后在访问实例context中调用。

C、SSLVPN访问实例context及其他配置：

```
sslvpn context test
gateway gw_test2
ip-tunnel interface SSLVPN-AC1
ip-tunnel address-pool sslvpn-pool mask 255.255.255.0
ip-route-list sslvpn
include XXX.100.56.0 255.255.255.0
include XXX.100.58.0 255.255.255.0
policy-group sslvpn
filter ip-tunnel acl 3333
ip-tunnel access-route ip-route-list sslvpn
default-policy-group sslvpn
aaa domain sslvpn
service enable #
```

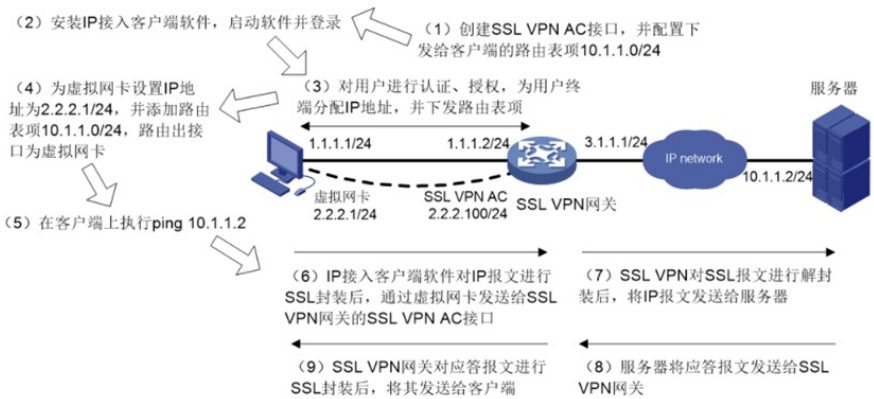
2、检查终端与设备公网口通信是否正常：公网网络正常，端口可用。





3、通过在防火墙web页面抓包检查报文交互过程：

正常的IP接入方式流程为：



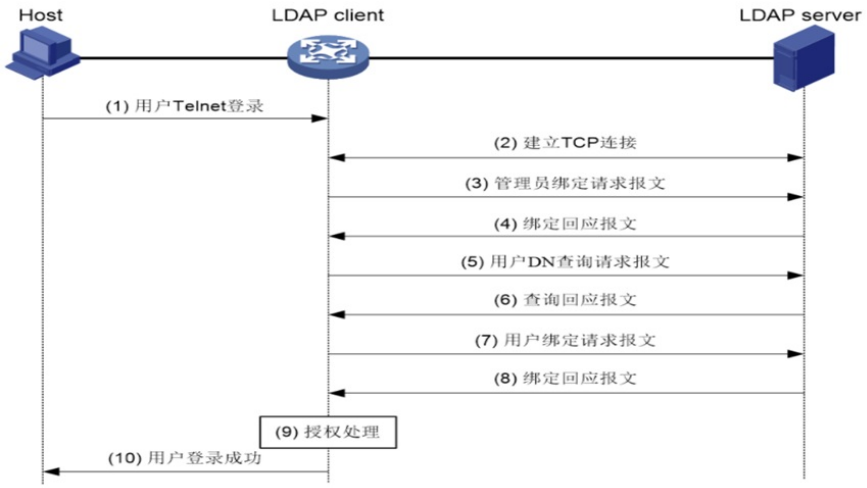
远程主机上通过iNode安装一个虚拟网卡，拨入后先进行SSL标准协议的交互，SSL交互过程：

```
Client                                          Server

ClientHello                  -------->
                                                ServerHello
                                                Certificate*
                                                ServerKeyExchange*
                                                CertificateRequest*
                                                ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     -------->
                                          [ChangeCipherSpec]
                             <--------             Finished
Application Data             <-------->     Application Data
```

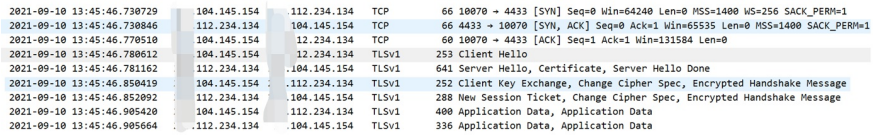
将接口的dns server XXX.177.7.1配置删除后问题解决。在配置sslvpn结合ldap时需要注意，接口上面配置dns server会和ldap域冲突，导致ldap认证时，会向dns服务器请求LDAP服务器的域名，导致设备认为查找用户失败，不进入下一步的绑定用户。

正常的LDAP认证交互流程（在上诉流程的第三步进行认证）：



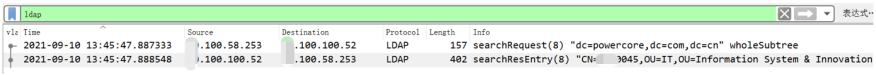
测试PC(XXX.104.145.154)—公网—(XXX .112.234.134:9527) **F1000-AI-60**(XXX .100.58.253)---(XXX .100.100.52)**LDAP服务器**

SSL过程抓包显示出SSL交互过程正常



2021-09-10 13:45:46.730729	104.145.154	112.234.134	TCP	66	10070 → 4433 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 WS=256 SACK_PERM=1
2021-09-10 13:45:46.730846	112.234.134	104.145.154	TCP	66	4433 → 10070 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
2021-09-10 13:45:46.770510	104.145.154	12.234.134	TCP	60	10070 → 4433 [ACK] Seq=1 Ack=1 Win=131584 Len=0
2021-09-10 13:45:46.780612	104.145.154	12.234.134	TLSv1	253	Client Hello
2021-09-10 13:45:46.781162	112.234.134	.104.145.154	TLSv1	641	Server Hello, Certificate, Server Hello Done
2021-09-10 13:45:46.850419	104.145.154	.112.234.134	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2021-09-10 13:45:46.852092	112.234.134	.104.145.154	TLSv1	288	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2021-09-10 13:45:46.905420	104.145.154	.112.234.134	TLSv1	400	Application Data, Application Data
2021-09-10 13:45:46.905664	.112.234.134	.104.145.154	TLSv1	336	Application Data, Application Data

LDAP认证过程：服务器回复了查询报文就没有后续交互的报文，设备并没有开始进一步的用户绑定请求。



No.	Time	Source	Destination	Protocol	Length	Info
2021-09-10 13:45:47.887333	.100.58.253	.100.100.52	LDAP	157	searchRequest(8) "dc=powercore,dc=com,dc=cn" wholeSubtree
2021-09-10 13:45:47.888548	.100.100.52	.100.58.253	LDAP	402	searchResEntry(8) "CN= 0045,OU=IT,OU=Information System & Innovation

4、通过debug进一步对SSL过程及LDAP认证过程进行分析（debugging sslvpn all 、debugging ldap all）：

现场LDAP用户信息： CN=XXX0045,OU=IT,OU=Information System & Innovation Center,OU=Powercore,DC=powercore,DC=com,DC=cn

SSL过程完整，但是LDAP认证过程查找用户过程异常。

PAM_LDAP:**User DN is CN=XXX0045,OU=IT,OU=Information System & Innovation Center,OU=Powercore,DC=powercore,DC=com,DC=cn. //查找用户DN**

*Sep 10 13:42:26:468 2021 H3C LDAP/7/EVENT: -COntext=1;

PAM_LDAP:**Keep state authentication searching for incomplete searching.**

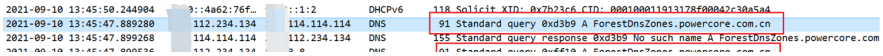
*Sep 10 13:42:34:635 2021 H3C LDAP/7/EVENT: -COntext=1;

PAM_LDAP**:Get result message errno = -14**

5、服务器与设备交互DN请求报文后，设备侧如果正常认证的话，会存在一个User XXX search done. ，状态才会从查询DN用户变为绑定用户。

那为什么设备会认为用户没有查询成功呢?

通过对抓包信息进一步分析，设备一直在向DNS服务器发送DNS报文，请求解析powercore.com.cn域名，这个对应的是LDAP所在域。由于真实网络不存在对应域名，DNS解析失败，因此可能设备会认为用户查询一直未成功。


2021-09-10 13:45:50.244904 9::4a62:76f… ::1:2 DHCPv6 118 Solicit XID: 0x7b23c6 CID: 000100011913178f00042c30a5a4
2021-09-10 13:45:47.889280 112.234.134 114.114.114 DNS 91 Standard query 0xd3b9 A ForestDnsZones.powercore.com.cn
2021-09-10 13:45:47.899268 114.114.114 112.234.134 DNS 155 Standard query response 0xd3b9 No such name A ForestDnsZones.powercore.com