V7防火墙使用默认证书配置SSL VPN LDAP认证典型案例（WEB配置）

SSL VPN　张新姿　2020-10-31 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：本案例适用于如F1000-A-G2、F1000-S-G2 、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P19版本上进行配置和验证的。

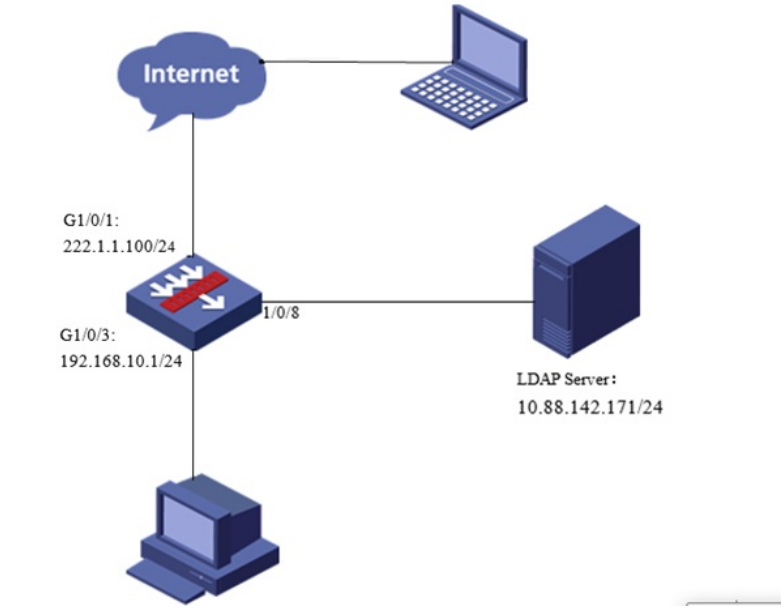
服务器系统：windows server 2012 R2

1.2 配置需求及实现的效果

V7防火墙部署在互联网出口，外网终端通过INode软件拨入SSL VPN，防火墙通过LDAP Server 对用户进行远程认证和授权。认证成功后用户可以访问内网192.168.10.0网段的资源。IP地址及接口规划如下表所示：

外网接口	公网地址/掩码	内网接口	内网地址/掩码	与LDAP互联口	LDAP服务器地址
GE1/0/1	222.1.1.100/24	GE1/0/3	192.168.10.1/24	GE1/0/8	10.88.142.171

2 组网图



配置步骤

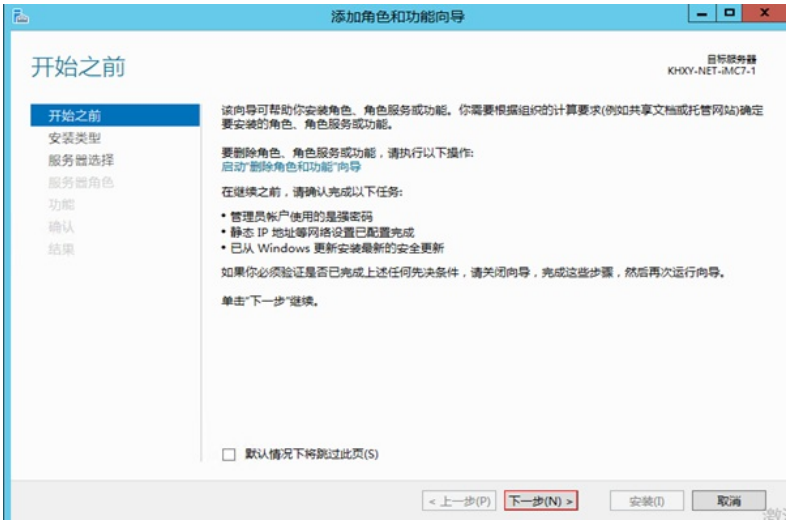
1.1 Windows server 2012镜像安装

请参考微软镜像安装手册或者百度自行解决，本文对Windows server 2012系统安装不做赘述。

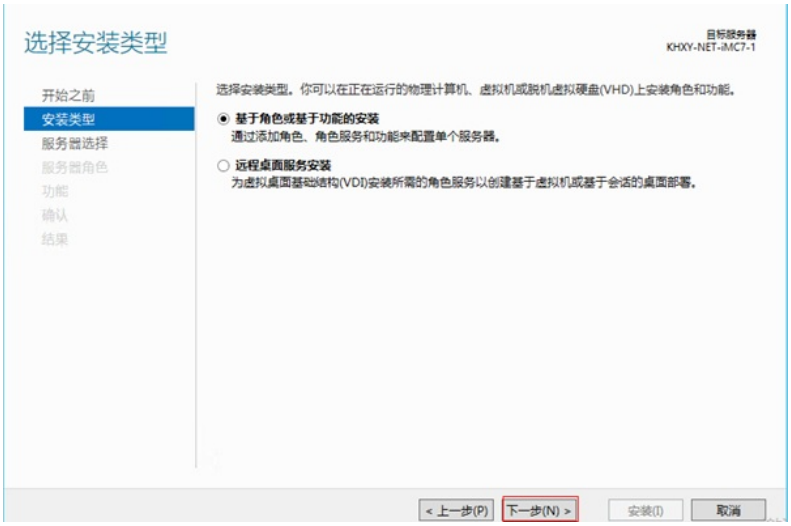
1.2 LDAP服务器设置

1、在服务器界面点击“开始”旁边的服务器管理器按钮，调出管理器界面后点击“添加角色和功能选项”。

2、在出现的角色和功能向导中点击下一步。

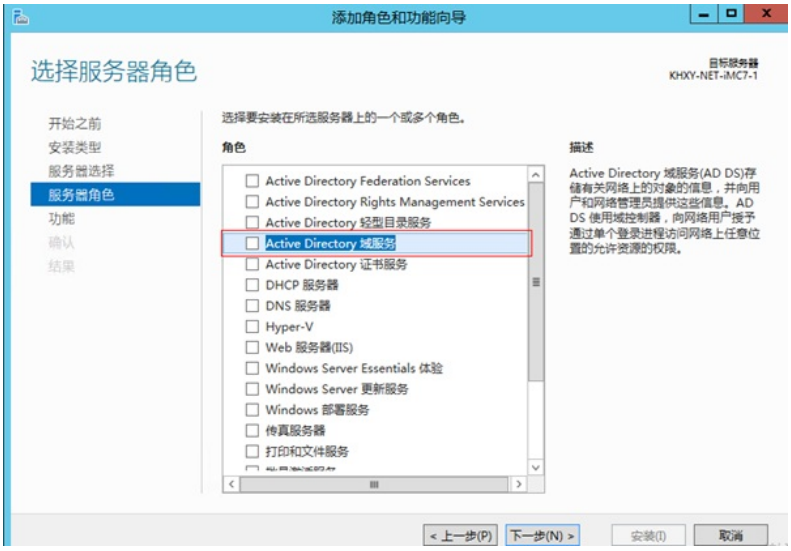


3、安装类型选择“基于角色或基本功能的安装”后点击下一步。



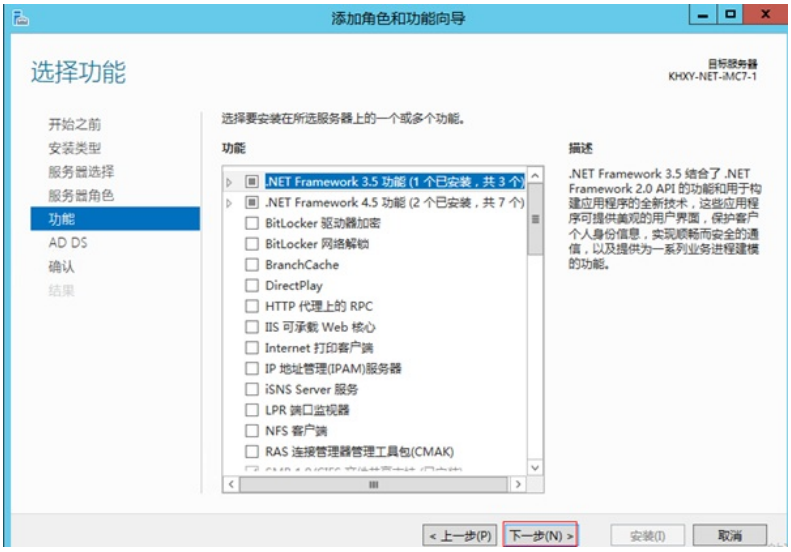
4、服务器选择显示为本机地址的服务器。

5、在服务器角色中点击Active Directory 域服务。

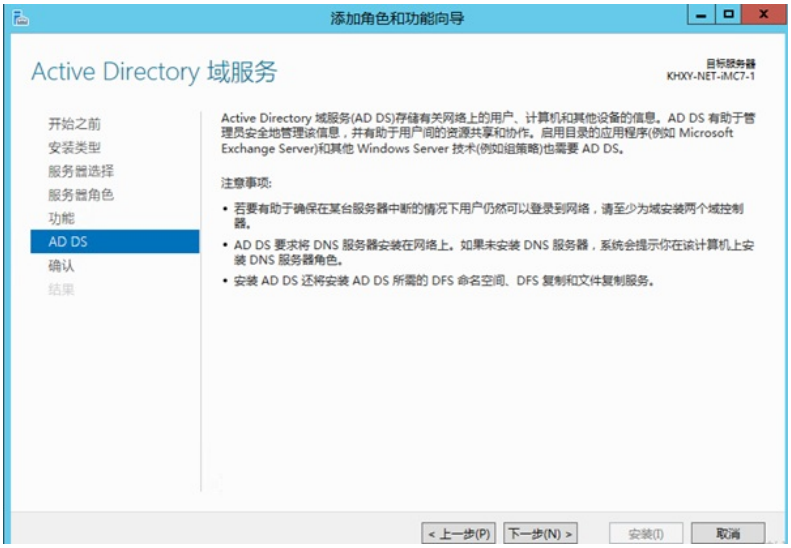


在点击过程中会弹出新的对话框，点击远程服务器管理工具后选择添加功能。

6、如果没有特殊需要不需要选择任何功能直接点击下一步即可。



7、出现Active Directory 域服务点击下一步。

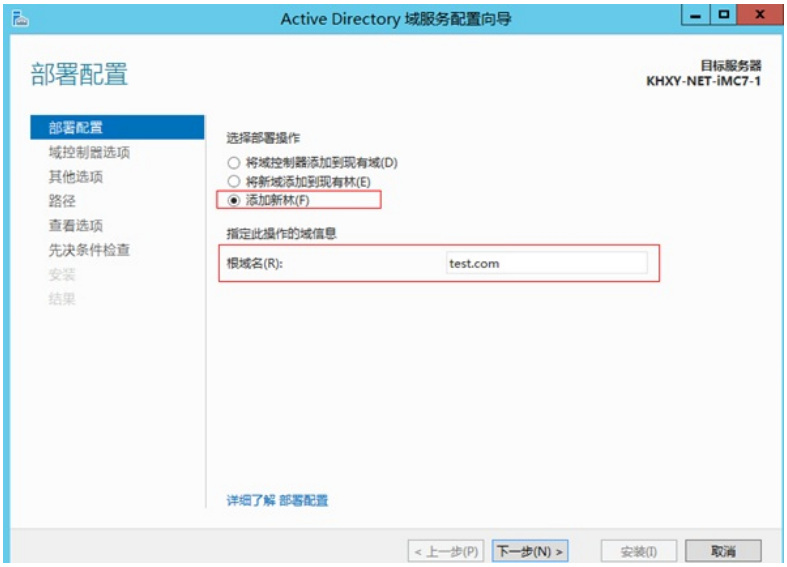


8、确认无误后点击安装Active Directory 域服务程序，安装成功后关闭向导。

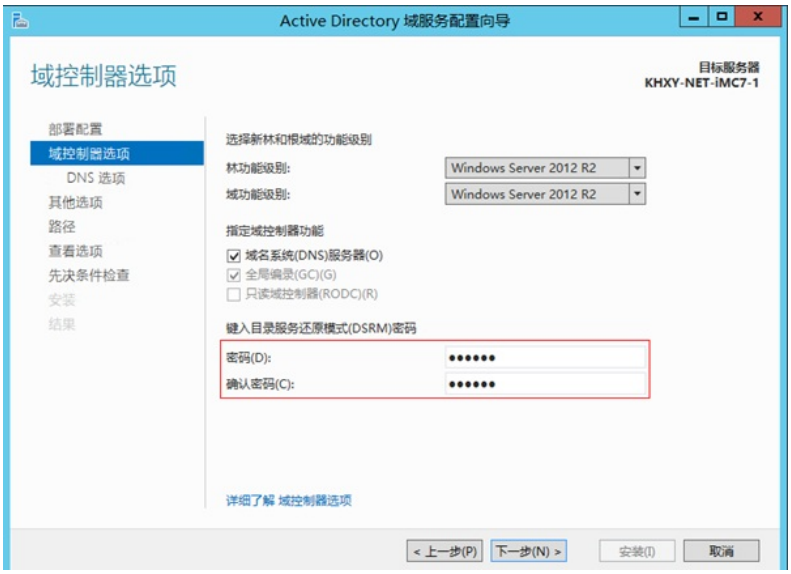
9、服务器部署成功后出现AD DS选项，点击"更多"打开域配置界面。

10、点击"将此服务器提升为域控制器"选项。

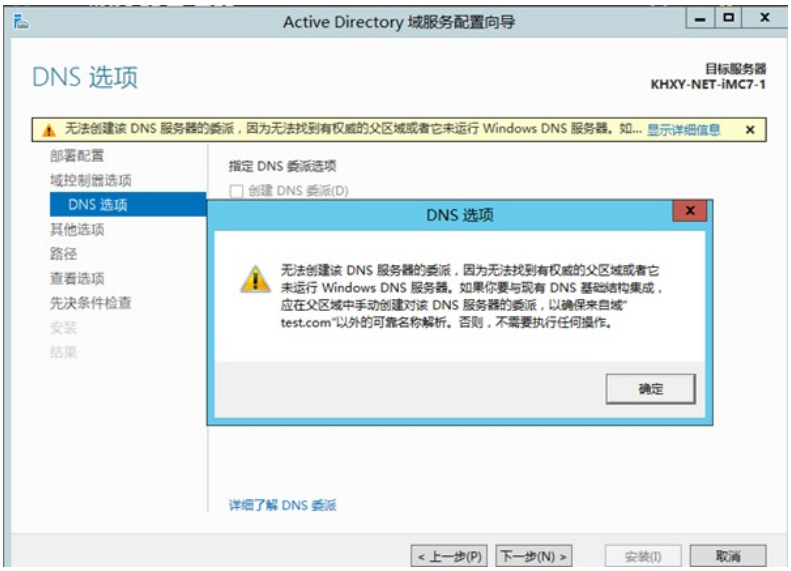
11、选择添加新林并且将根域名设置为test.com。



12、创建目录服务还原密码后点击下一步。

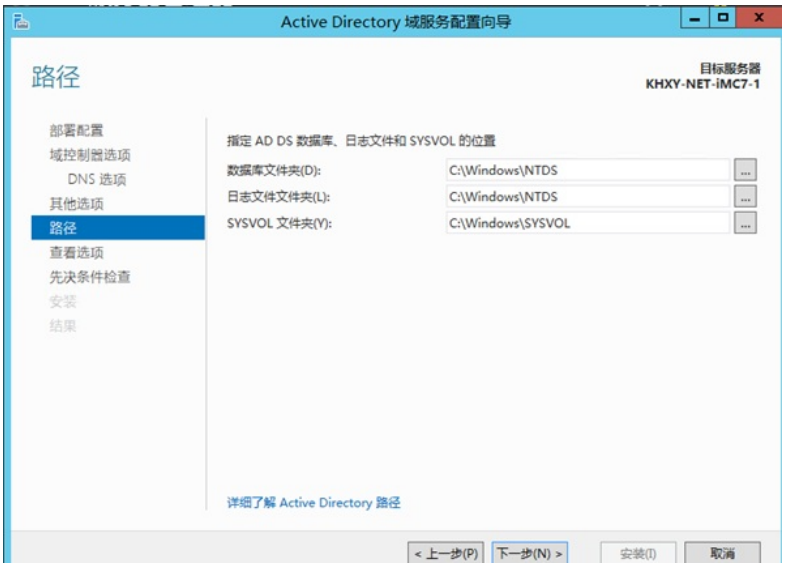


13、在DNS选项设置中会出现报错无法创建DNS服务器，可以忽略直接下一步即可。



14、设置NetBIOS域名，系统已经根据根域默认为TEST不用修改点击下一步。

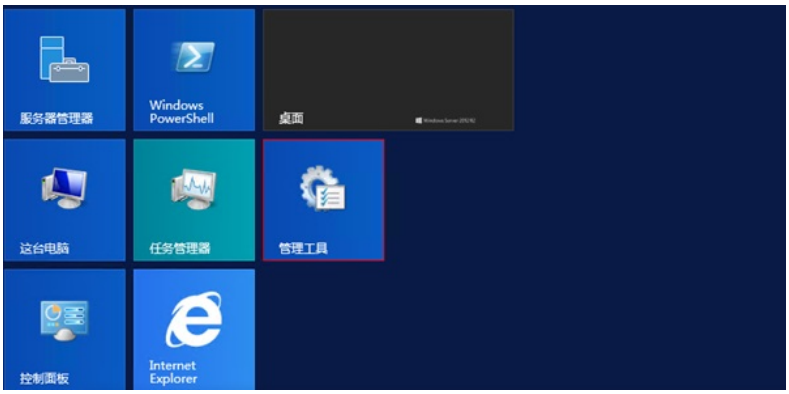
15、选择数据库、日志、SYSVOL文件夹的目录。



16、检查选项无误后选择下一步。

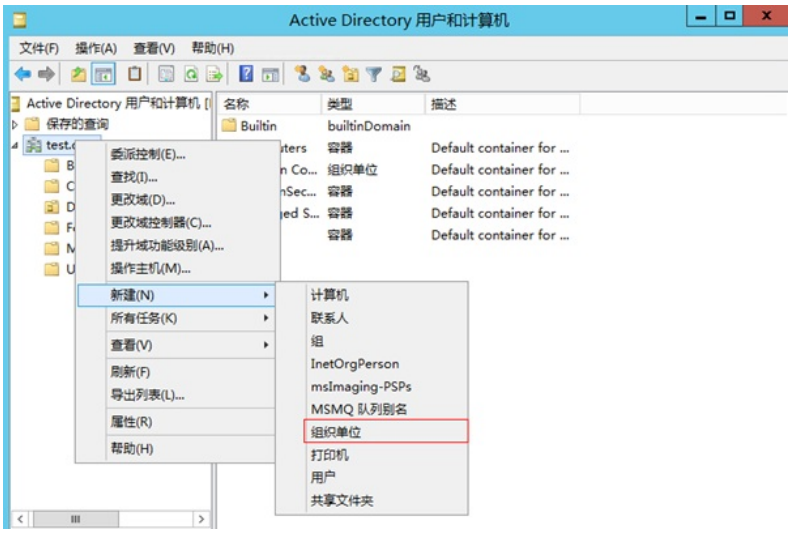
17、先决条件检查完成后选择安装，安装完成后点击关闭，关闭需要重启服务器后域名系统才能正常工作。

18、开启开启后选择管理工具。

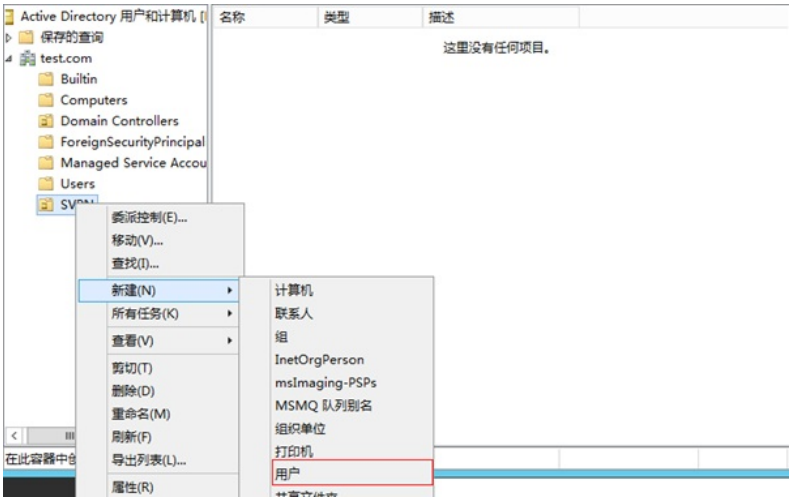


19、点击Active Directory 用户和计算机

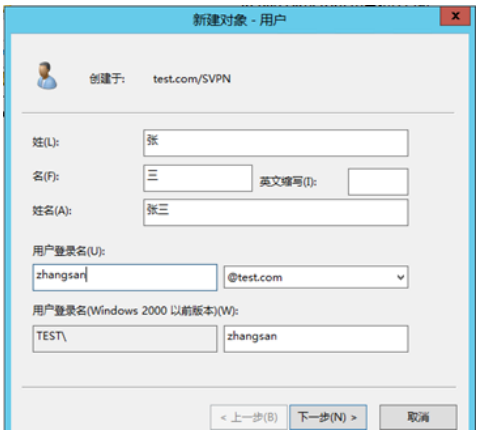
20、新建一个SVPN的组织单位用来存储SSL VPN用户。



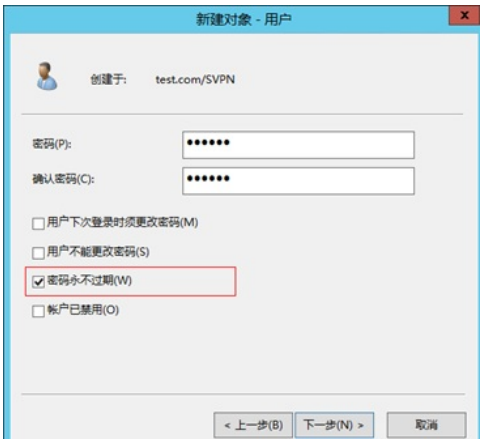
21、在SVPN组中添加用户



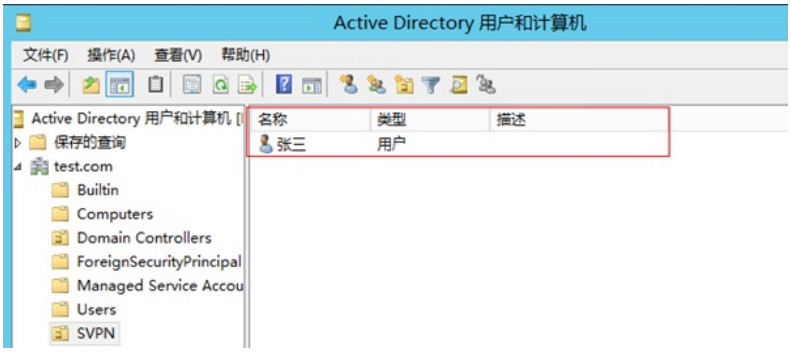
22、添加用户为张三设置登录账号为zhangsan。



23、设置密码并设置密码为永不过期。



24、设置完成后出现张三用户，至此LDAP服务器所有配置完成。



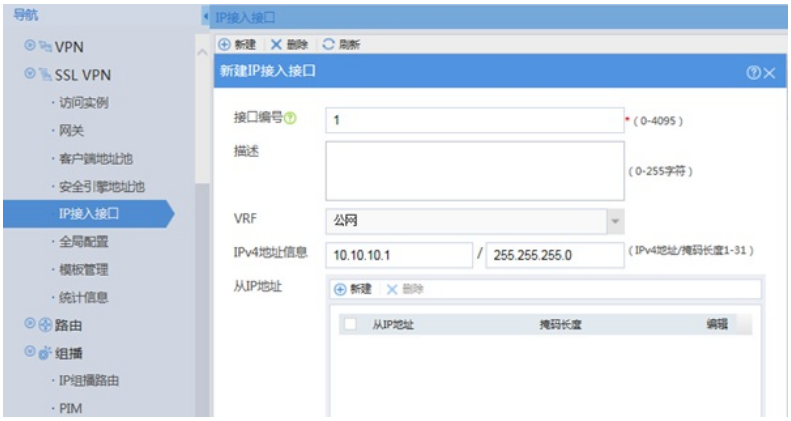
1.3 防火墙侧配置

1.3.1 配置SSL VPN网关

#选择 “网络”>“SSL VPN”>“网关”点击”新建”，IP地址填写防火墙GE1口地址222.1.1.100，端口号修改为4433（缺省SSL VPN也是443端口与设备WEB登录端口冲突），勾选“使能”选项点击“确定”完成配置。

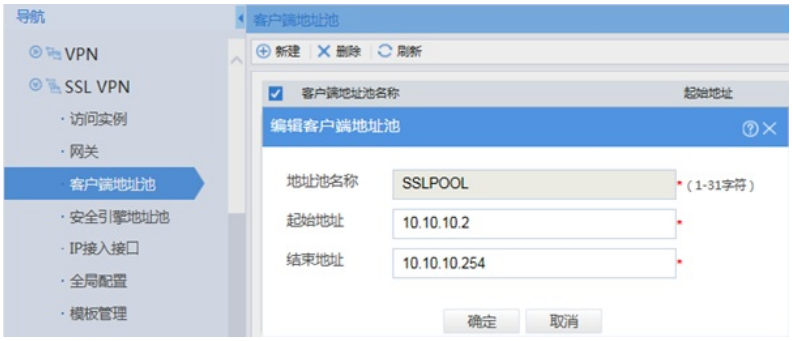
1.3.2 增加SSL VPN接入接口

#点击 “网络”>“SSL VPN”>“IP接入接口”后新建IP接入接口，接口编号配置为1、IPV4地址配置为10.10.10.1/24。



1.3.3 增加客户端地址池

#点击 “网络”>“SSL VPN”>“客户端地址池”新建客户端地址池，地址池名配置为“SSLPOOL”、起始地址配置为10.10.10.2、结束地址配置为10.10.10.254，配置完成后点击确定。



1.3.4 配置SSL VPN访问实例

#点击 “网络”>“SSL VPN”>“访问实例”中新建访问实例，在“关联网关”中点击新建关联3.3.1创建的SSL VPN网关，在ISP域中添加ISP认证域，认证域名称配置为“svpn”其他选项全部为默认，配置完成后点击确定。

1.3.5 配置SSL VPN访问实例中的IP业务

#点击 “网络”>“SSL VPN”>“访问实例”>“IP业务”IP接入接口选择3.3.2步骤添加的接口1（SSLVPN-AC1）、客户端地址池选择3.3.3步骤添加的“SSLPOOL”、配置客户端掩码及主DNS服务器地址分别为24和114.114.114.114后点击页面下方确定完成配置。

#在页面下面的IP接入资源中点击“新建”创建名称为NEIWANG的路由列表，然后在该路由列表中继续

新建组网地址为192.168.10.0/24的内网资源，当SSL VPN用户拨入后可以直接访问该网段下的所有资源。

1.3.6 配置SSL VPN访问实例中的资源组

#点击 “对象”>“ACL”>“IPv4”中新建高级ACL编号为3999，点击确定进入规则配置。

进入规则配置界面后IP协议类型选择ip、取消继续添加下一条规则选项后点击确定完成配置。

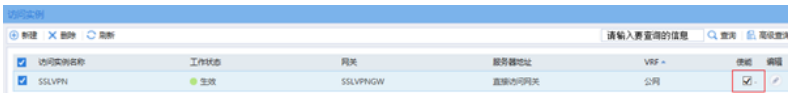
1.3.7 配置SSL VPN访问实例中的资源组

#点击 “网络”>“SSL VPN”>“访问实例”>“资源组”中新建名称为SSLVPNZIYUAN的资源组，

在指定路由接入VPN中选择子网资源、子网资源选择3.3.5步骤创建的资源NEIWANG、IPV4 ACL用于控制SSL VPN接入用户，选择3.3.6步骤创建IPv4 ACL 3999点击确定完成配置。

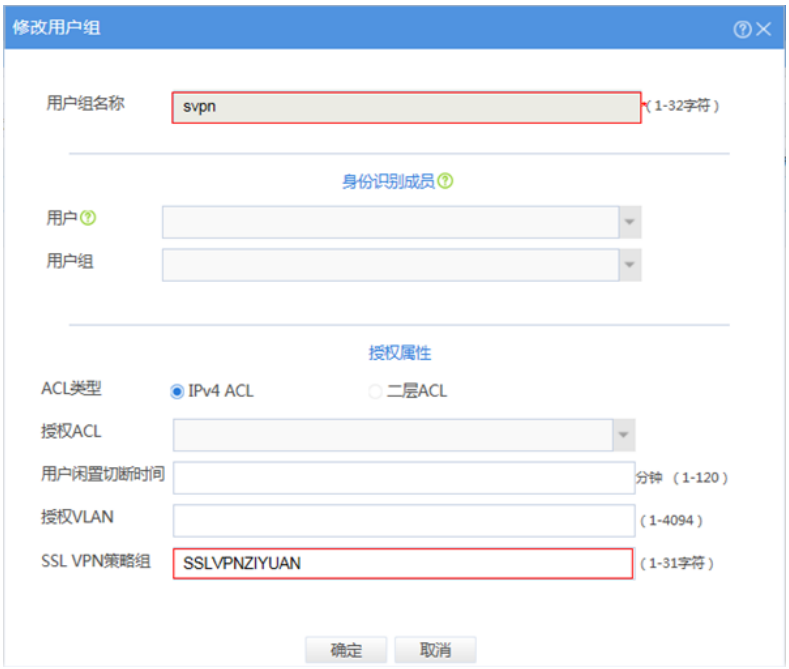
1.3.8 配置SSL VPN访问实例中的资源组

#在 “网络”>“SSL VPN”>“访问实例”中点击使能开启SSL VPN实例。



1.3.9 创建SSL VPN用户组

#在 “对象”>“用户”>“用户管理”>“本地用户”>“用户组”中新建名称为svpn的用户组，在SSL VPN策略组中将3.3.7步骤中创建的SSLVPNZIYUAN组调用在该用户组。



1.3.10 创建LDAP服务器

#在 “对象”>“用户”>“认证管理”>“LDAP”>“LDAP方案”新建名称为svpn的LDAP认证方案。

配置LDAP服务器名称为svpn、LDAP服务器地址为10.88.142.171、管理员DN为cn=administrator,cn=users,dc=test,dc=com、管理员密码为administrator用户密码、用户DN查询的起点为ou=svpn,dc=test,dc=com、用户名属性为samaccountname。对于上述所有参数的解释说明：login-dn是LDAP管理账号的路径（要求此管理账号有读权限或者管理员权限）、管理员密码对应administrator账号的密码、search-base-dn表示要查找的用户所在的目录、user-parameters samaccountname参数表示查找用户属性samaccountname值，设备默认查询用户属性查询CN值。

1.3.11 创建LDAP方案（需在命令行完成）

创建LDAP方案将LDAP认证和授权全部指向3.3.10步骤中创建的LDAP服务器。

[H3C]ldap scheme svpn

[H3C-ldap-svpn]authentication-server svpn

[H3C-ldap-svpn]authorization-server svpn

1.3.12 创建SSL VPN认证域（需在命令行完成）

创建SSL VPN认证域，将认证授权全部改向3.3.11步骤创建的svpn方案，并且指定3.3.9步骤中创建的认证用户组svpn。

[H3C]domain svpn

[H3C-isp-svpn]authorization-attribute user-group svpn

[H3C-isp-svpn]authentication sslvpn ldap-scheme svpn

[H3C-isp-svpn]authorization sslvpn ldap-scheme svpn

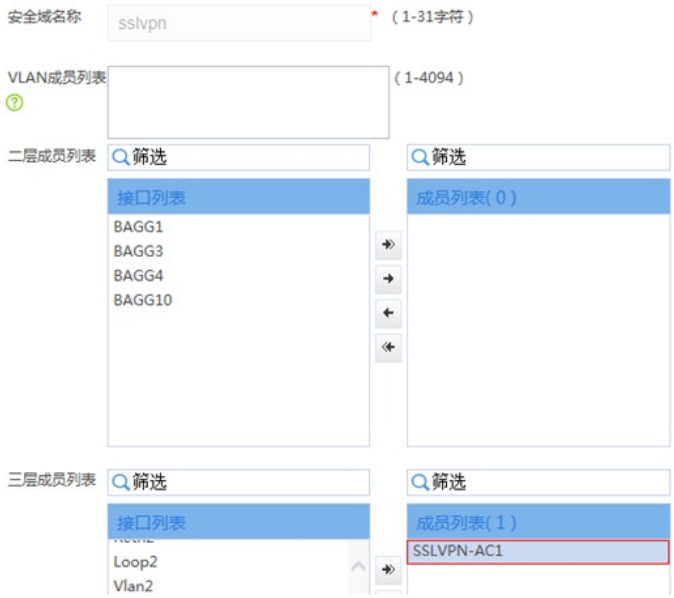
[H3C-isp-svpn]accounting sslvpn none

1.3.13 配置与LDAP服务器互联端口

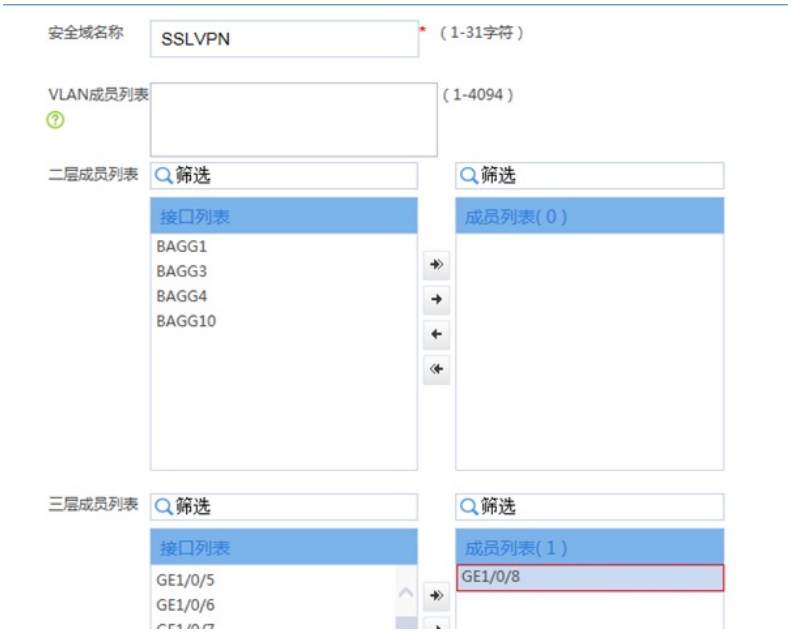
#在 “网络”>“IP”找到1/0/8接口并配置1/0/8接口地址为10.88.142.1掩码配置为255.255.255.0。

1.3.14 将SSL VPN端口加入安全域，放通对应安全策略

#在 “策略”>“安全域”中新建名称为SSLVPN的安全域，将步骤3.3.2添加的SSLVPN-AC1接口添加到SSLVPN域。



#在 “策略”>“安全域”中新建名称为LDAP的安全域，将步骤3.3.13添加的与LDAP服务器互联接口GE1/0/8添加到LDAP域。



#在 “对象”>“服务对象组”中新建名称为4433的对象组，点击页面中添加按钮后将目的端口设置起始端口和结束端口都设置为4433（3.3.1步骤中SSL VPN网关的端口）。

#在 “策略”>“安全策略”中将Untrust到Local域目的端口为TCP4433端口放通。

#配置配置安全策略放通源安全域为SSLVPN，目前安全域为“Trust”的数据流量

#配置配置安全策略,放通安全域为DMZ、Local域的数据流量。（点击多选按钮可以选择多个安全域）

1.4 保存配置

1.5 配置验证，查看拨号成功的用户

可以在WEB界面SSL VPN统计信息中查看SSL VPN拨入信息，也可以在命令行通过dis sslvpn session verbose查看用户信息。

dis sslvpn session verbose

User : zhangsan

Context : SSLVPN

Policy group : SSLVPNZIYUAN

Idle timeout : 30 min

Created at : 19:52:36 UTC Sun 04/19/2020

Lastest : 19:52:36 UTC Sun 04/19/2020

User IPv4 address : 10.88.26.145

Alloced IP : 10.10.10.2

Session ID : 14

Web browser/OS : Windows

客户端使用INode登录截图：

配置关键点

注意事项

1、安装Active Directory后服务器所在域会变更导致重启后无法使用原账号登录，登录时需要使用“域名\用户名”的方式去登录。

2、因为设备默认查询用户属性是查询CN值，当LDAP服务器用户名与登录账号不一致情况下需要设备查询samaccountname值来确定用户登录名，因此在设备LDAP Server下“user-parameters user-name-attribute samaccountname”命令是一定要添加的。