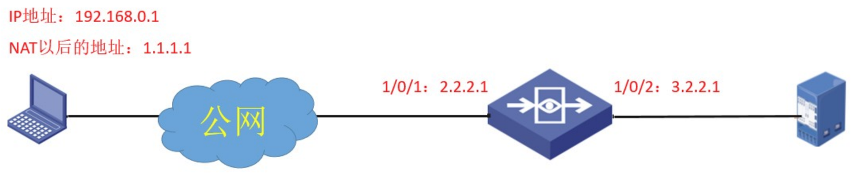
L2TP over IPSEC 在NAT穿越下的配置

L2TP over IPSec VP　**孔梦龙**　2021-05-14 发表

组网及说明



防火墙设备做LNS，客户端集成LAC

配置步骤

1、接口加入安全域，放通相应的安全策略

2、 防火墙的接口配置如下：

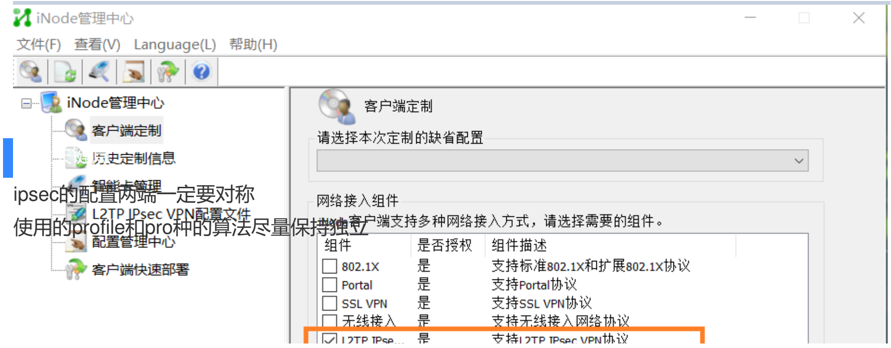
```
interface GigabitEthernet1/0/1
 port link-mode route
 description 移动 bandwidth 102400
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy l2tp
```

3、防火墙的L2TP/IPSEC 配置

```
#
 ip pool 10 172.16.1.10 172.16.1.100        //LNS给远端分配地址的地址池
#
interface Virtual-Template1
 ppp authentication-mode chap pap
 remote address pool 10
 ip address 172.16.1.1 255.255.255.0        //VT口的地址是172.16.1.1，认证远端的方式是CHAP或PAP
#
local-user root class network
 password simple root
 service-type ppp
 authorization-attribute user-role network-operator     //配置登录的用户，用户类型为PPP，账户密码均为root
#
ipsec transform-set 1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1                  //配置使用的transform的类型
#
ipsec policy-template l2tp 10
 transform-set 1
 ike-profile 1
 reverse-route dynamic              //配置IPSEC的策略
#
ipsec policy l2tp 10 isakmp template l2tp      //引用模板
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication            //配置本端为LNS
#
l2tp enable
#
ike profile 1
 keychain 10
 local-identity fqdn fw
 match remote identity fqdn client
 match local address GigabitEthernet1/0/1    //配置ipsecs使用的profile      注意和客户端一致
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5        //ipsec的提议                    注意和客户端一致
 #
ike keychain 10
 match local address GigabitEthernet1/0/1
 pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
#
```

inode的配置

1、定制inode客户端



客户端定制

请选择本次定制的缺省配置

网络接入组件

iNode客户端支持多种网络接入方式，请选择需要的组件。

组件	是否授权	组件描述
□ 802.1X	是	支持标准802.1X和扩展802.1X协议
□ Portal	是	支持Portal协议
□ SSL VPN	是	支持SSL VPN协议
□ 无线接入	是	支持无线接入网络协议
☑ L2TP IPse...	是	支持L2TP IPsec VPN协议

ipsec的配置两端一定要对称

使用的profile和pro种的算法尽量保持独立