防火墙L2TP over IPSec典型配置

L2TP over IPSec VP 孔凡安 2021-12-27 发表

组网及说明

实验环境，为方便配置，设定隧道两端直连。
现网环境可能涉及到NAT转换，跨越公网等情况，以此为参考即可。
本案例不涉及安全域和安全策略的说明，策略默认any-any。

配置步骤

防火墙配置：

注：防火墙与PC互联的接口为GigabitEthernet1/0

1. L2TP部分

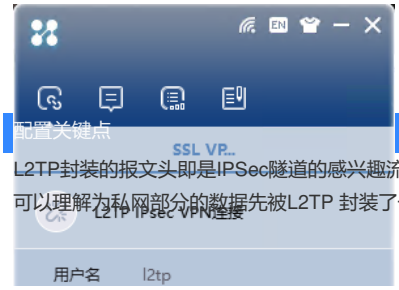
```
#
 l2tp enable
#
ip pool l2tp 10.10.1.4 10.10.1.10
ip pool l2tp gateway 10.10.1.3
#
interface Virtual-Template1   //创建接口Virtual-Template1，PPP认证方式为CHAP，并使用地址池l2tp为LAC client端分配IP地址
 ppp authentication-mode chap domain system
 remote address pool l2tp
 ip address 10.10.1.3 255.255.255.0
#
local-user l2tp class network       //创建l2tp登录的用户
 password cipher $c$3$MCLrk5FDm7c5UOHsGo0Br5FXnPQGmZYJbg==
 service-type ppp authorization-attribute
 user-role network-operator
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication  //关闭隧道验证功能
 tunnel name lns
```

2. IPsec部分

```
#
acl advanced 3100 rule 0 permit ip source 111.3.3.1 0 destination 111.3.3.254 0   //感兴趣流
#
ike keychain key
 pre-shared-key address 111.3.3.254 255.255.255.255 key cipher $c$3$UGr3MLpcFIvrmcHfJ4Sq5r1DjIfYp/BPTg==
#
ike profile pf
 keychain key
 dpd interval 10 retry 30 on-demand    //配置DPD检测
 local-identity address 111.3.3.1
 match remote identity address 111.3.3.254 255.255.255.255
#
ipsec transform-set ts
 esp encryption-algorithm
 3des-cbc esp authentication-algorithm md5
#
ipsec policy ply 1 isakmp
 transform-set ts
 security acl 3100
 remote-address 111.3.3.254
 ike-profile pf
#
interface GigabitEthernet1/0
 port link-mode route
 description l2tp&ipsec
 ip address 111.3.3.1 255.255.255.0
 ipsec apply policy ply
```

客户端配置：

注：客户端使用定制的inode智能客户端，如下：



配置关键点

L2TP封装的报文头即是IPSec隧道的感兴趣流。

可以理解为私网部分的数据先被L2TP 封装了一层公网头部，后被IPSec封装了一次公网头部。