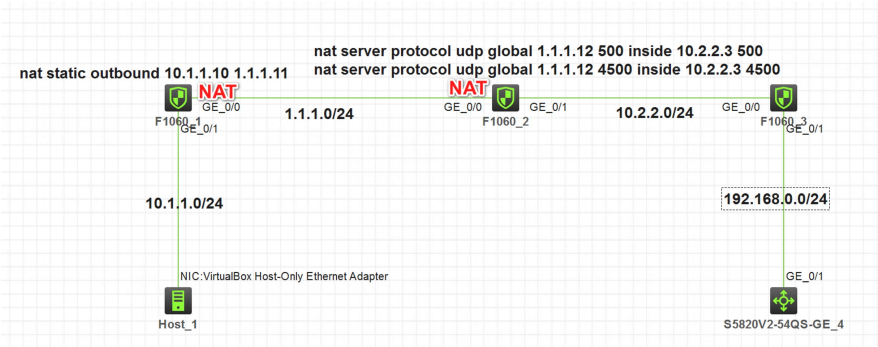
客户端iNode拨号 L2TP over IPsec 模拟器环境

L2TP over IPSec VP　孔凡安　2022-11-09 发表

组网及说明

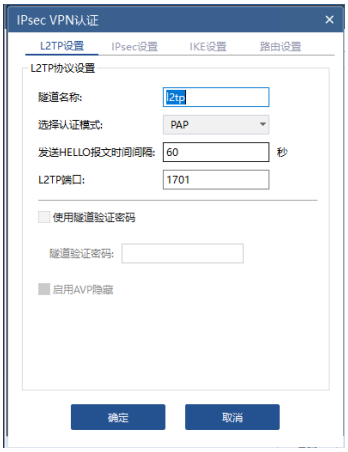


注：如无特别说明，描述中的 FW1 或 MSR1 对应拓扑中设备名称末尾数字为 1 的设备，FW2 或 MSR2 对应拓扑中设备名称末尾数字为 2 的设备，以此类推；另外，同一网段中，IP 地址的主机位为其设备编号，如 FW1 的 g0/0 接口若在 1.1.1.0/24 网段，则其 IP 地址为 1.1.1.1/24，以此类推。

实验说明：

1. FW1和FW2均为NAT设备，FW3为内网防火墙，外部FW上做了针对UDP500和4500端口的映射
2. FW3为LNS设备
3. SW4为内网服务器
4. 不涉及安全域和安全策略的配置，缺省全部放通

配置步骤

	FW3	Host
地址、路由、安全策略	# interface GigabitEthernet1/0/0 port link-mode route combo enable copper ip address 10.2.2.3 255.255.255.0 ipsec apply policy ply # interface GigabitEthernet1/0/1 port link-mode route combo enable copper ip address 192.168.0.3 255.255.255.0 # security-zone name Trust import interface GigabitEthernet1/0/1 import interface Virtual-Template1 # security-zone name Untrust import interface GigabitEthernet1/0/0 # ip route-static 0.0.0.0 0 10.2.2.2 # security-policy ip rule 0 name any action pass	C:\Users\Administrator>route add 1.1.1.12 mask 255.255.255.255 10.1.1.1 C:\Users\Administrator>route add 10.2.2.3 mask 255.255.255.255 10.1.1.1
L2TP部分	# ip pool aaa 192.168.200.2 192.168.200.250 ip pool aaa gateway 192.168.200.1 # interface Virtual-Template1 ppp authentication-mode pap domain system ppp ipcp dns 114.114.114.114 remote address pool aaa ip address 192.168.200.1 255.255.255.0 # domain system authorization-attribute ip-pool aaa authentication ppp local accounting ppp local # local-user l2tp class network password cipher c3$AbdCFddrmyOZSo++Rv5gkdMmtE4RA4Hhgw== service-type ppp authorization-attribute user-role level-15 authorization-attribute user-role network-operator # l2tp-group 1 mode lns allow l2tp virtual-template 1 undo tunnel authentication tunnel name l2tp # l2tp enable	
IPsec	# interface GigabitEthernet1/0/0 port link-mode route combo enable copper ip address 10.2.2.3 255.255.255.0 ipsec apply policy ply # ipsec transform-set 1 encapsulation-mode transport esp encryption-algorithm 3des-cbc esp authentication-algorithm md5 # ipsec transform-set 2 encapsulation-mode transport esp encryption-algorithm aes-cbc-128 esp authentication-algorithm sha1 # ipsec transform-set 3 encapsulation-mode transport esp encryption-algorithm aes-cbc-256 esp authentication-algorithm sha1 # ipsec transform-set 4	

配置关键点

1. 客户端Host需要手动添加路由，不然报错的报文可能从电脑的其他网卡出去。
2.开启IPsec反向路由注入功能，开启后在FW3上查看去往Host网段的路由如下：

```
<H3C>disp ip rou 10.1.1.10

Summary count : 2

Destination/Mask  Proto  Pre  Cost      NextHop         Interface
0.0.0.0/0         Static 60   0         10.2.2.2        GE1/0/0
10.1.1.10/32      Static 60   0         1.1.1.11        GE1/0/0
```

```
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 5
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 6
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec transform-set 7
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
ipsec transform-set 8
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec transform-set 9
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set 10
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 11
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 12
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec transform-set l2tp
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy-template pt 1
 transform-set 3 4 5 7 8 9
 ike-profile pf
 reverse-route dynamic
#
ipsec policy ply 1 isakmp template pt
#
ike profile pf
 keychain 1
 exchange-mode aggressive
 local-identity fqdn lns
 match remote identity fqdn lac
 match remote identity address 0.0.0.0 0.0
.0.0
 proposal 1 2 3 4 5 6
#
ike proposal 1
 encryption-algorithm aes-cbc-128
 dh group2
 authentication-algorithm md5
#
ike proposal 2
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike proposal 3
 encryption-algorithm 3des-cbc
 dh group2
#
ike proposal 4
 encryption-algorithm aes-cbc-256
 dh group2
#
ike proposal 5
 dh group2
#
ike proposal 6
 encryption-algorithm aes-cbc-192
 dh group2
#
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 k
ey cipher $c$3$zJ43hnEq21nU56zR2GjA
ny9C1I+e8x8FPw==
```