拓扑：

192.168.2.0/24（无线网段）---192.168.1.0----(mgt1--192.168.1.143) KFW(mgt2--192.168.101.1) -----192.168.101.0-----Internet

VPN分配的地址段 192.168.200.1--192.168.200.20

防火墙配置

vpn配置

define vpn ipsec phase1

 edit "p1"

 set type dynamic

 set interface "mgt1" 选择内网接口

 set dhgrp 2 5 14

 set proposal aes256-md5 aes128-sha1

 set localid-type address

 set psksecret 12345678

 next

end



阶段2配置

define vpn ipsec phase2

 edit "p2"

 set encapsulation transport-mode （这个是在图形界面没有配置，需要命令行设置）

 set keylife-type both

 set pfs disable

 set phase1name "p1"

 set proposal aes256-md5 aes128-sha1

 set keylifekbs 4608000

 set keylifeseconds 3600

 next

end



l2tp设置

define vpn l2tp

 set eip 192.168.200.20

 set sip 192.168.200.1

 set status enable

 set dns-server1 114.114.114.114

 set usrgrp "t"

end

策略设置

IPsec策略 从外网到内网建策略，动作是IPsec, 选择vpn隧道



允许客户端访问外网策略，从内网到外网建NAT策略。

