1. 实验需求

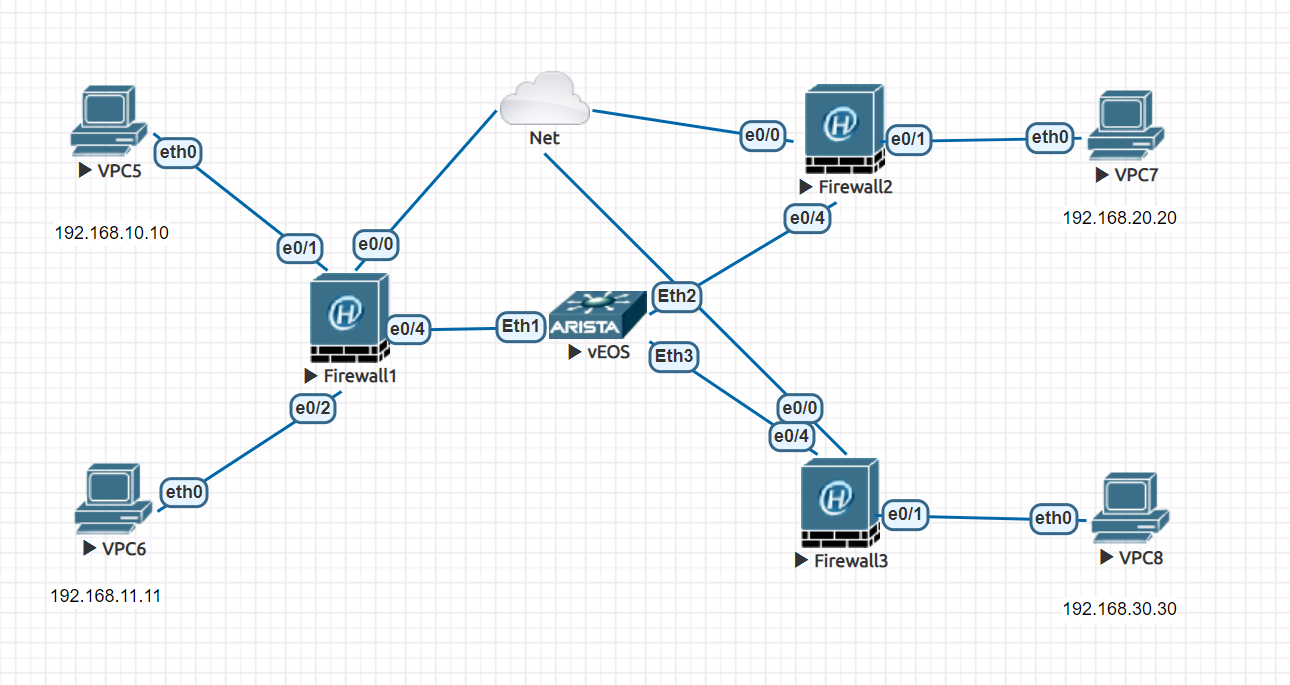
需求一:所有的VPC都能够访问到ISP

需求二:要求VPC6能够访问到VPN4，不能访问VPC5

需求三:要求VPC7能够访问VPC456

以上需求通过IPSEC实现

1. 实验拓扑



1. 实验步骤

步骤一：完成防火墙和交换机的基本配置；

|  |
| --- |
| # 交换机SW1配置  localhost#configure  localhost(config)#interface e1  localhost(config-if-Et1)#no switchport  localhost(config-if-Et1)#ip add 200.1.1.254/24  localhost(config-if-Et1)#interface e2  localhost(config-if-Et2)#no switchport  localhost(config-if-Et2)#ip add 100.0.0.254/24  localhost(config-if-Et2)#interface e3  localhost(config-if-Et3)#no switchport  localhost(config-if-Et3)#ip add 101.0.0.254/24  localhost(config-if-Et3)#exi  localhost(config)#ip routing  localhost(config)#show ip route  Codes: C - connected, S - static, K - kernel,  O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,  E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,  N2 - OSPF NSSA external type2, B I - iBGP, B E - eBGP,  R - RIP, I - ISIS, A B - BGP Aggregate, A O - OSPF Summary,  NG - Nexthop Group Static Route  Gateway of last resort is not set  C 100.0.0.0/24 is directly connected, Ethernet2  C 101.0.0.0/24 is directly connected, Ethernet3  C 200.1.1.0/24 is directly connected, Ethernet1  # 防火墙FW1配置  SG-6000# conf  SG-6000# configure  SG-6000(config)# hostname FW1  2022-05-12 07:10:12, Event WARNING@MGMT: Hostname is changed to FW1  FW1(config)# inte  FW1(config)# interface e0/4  FW1(config-if-eth0/4)# zone u  FW1(config-if-eth0/4)# zone untrust  FW1(config-if-eth0/4)# ip add 200.1.1.1/24  FW1(config-if-eth0/4)# manage ping  FW1(config-if-eth0/4)# ping 200.1.1.254  Sending ICMP packets to 200.1.1.254  Seq ttl time(ms)  1 64 49.6  2 64 5.76  3 64 9.04  4 64 9.30  5 64 8.85  statistics:  5 packets sent, 5 received, 0% packet loss, time 4005ms  rtt min/avg/max/mdev = 5.769/16.525/49.662/16.618 ms  FW1(config-if-eth0/4)# exi  FW1(config)# inter  FW1(config)# interface e0/1  FW1(config-if-eth0/1)# zone tr  FW1(config-if-eth0/1)# zone trust  FW1(config-if-eth0/1)# ip add 192.168.10.1/24  FW1(config-if-eth0/1)# manage  FW1(config-if-eth0/1)# manage ping  FW1(config-if-eth0/1)# exi  FW1(config)# inter  FW1(config)# interface e0/2  FW1(config-if-eth0/2)# zone tru  FW1(config-if-eth0/2)# zone trust  FW1(config-if-eth0/2)# ip add 192.168.11.1/24  FW1(config-if-eth0/2)# manage ping  FW1(config-if-eth0/2)# exi  FW1(config)# show ip rou  FW1(config)# show ip route  Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,  B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, V - VPN, M - IMPORT,  I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, \* - FIB route, b - BFD enable  Routing Table for Virtual Router <trust-vr>  ==============================================================================  S>\* 0.0.0.0/0 [1/0/1] via 200.1.1.254, ethernet0/4  C>\* 192.168.10.0/24 is directly connected, ethernet0/1  H>\* 192.168.10.1/32 [0/0/1] is local address, ethernet0/1  C>\* 192.168.11.0/24 is directly connected, ethernet0/2  H>\* 192.168.11.1/32 [0/0/1] is local address, ethernet0/2  C>\* 192.168.121.0/24 is directly connected, ethernet0/0  H>\* 192.168.121.129/32 [0/0/1] is local address, ethernet0/0  C>\* 200.1.1.0/24 is directly connected, ethernet0/4  H>\* 200.1.1.1/32 [0/0/1] is local address, ethernet0/4  ==============================================================================  FW1(config)# show inter  FW1(config)# show interface  H:physical state;A:admin state;L:link state;P:protocol state;U:up;D:down;K:ha keep up;C:lacp down  ========================================================================================================  Interface name IP address/mask Zone name H A L P MAC address Description  --------------------------------------------------------------------------------------------------------  ethernet0/0 192.168.121.129/24 trust U U U U 5000.0001.0000 ------  ethernet0/1 192.168.10.1/24 trust U U U U 5000.0001.0001 ------  ethernet0/2 192.168.11.1/24 trust U U U U 5000.0001.0002 ------  ethernet0/3 0.0.0.0/0 NULL U U U D 5000.0001.0003 ------  ethernet0/4 200.1.1.1/24 untrust U U U U 5000.0001.0004 ------  vswitchif1 0.0.0.0/0 NULL D U D D 001c.5410.ba12 ------  ========================================================================================================  FW1(config)# ip vr  FW1(config)# ip vrouter tr  FW1(config)# ip vrouter trust-vr  FW1(config-vrouter)# ip rout  FW1(config-vrouter)# ip route 0.0.0.0/0 200.1.1.254  2022-05-12 07:12:40, Network INFO@NET: Route in VR trust-vr that has IP address 0.0.0.0/0 through nexthop 200.1.1.254 with precedence 1 is created  FW1(config-vrouter)# sna  FW1(config-vrouter)# snatrule from 19  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any ser  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any service any eif  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any service any eif e0/4 tra  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any service any eif e0/4 trans-to eif  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any service any eif e0/4 trans-to eif-ip mod  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any service any eif e0/4 trans-to eif-ip mode dy  FW1(config-vrouter)# snatrule from 192.168.0.0/16 to any service any eif e0/4 trans-to eif-ip mode dynamicport  rule ID=2  FW1(config-vrouter)# end  FW1# show ip rout  FW1# show ip route  Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,  B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, V - VPN, M - IMPORT,  I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, \* - FIB route, b - BFD enable  Routing Table for Virtual Router <trust-vr>  ==============================================================================  S>\* 0.0.0.0/0 [1/0/1] via 200.1.1.254, ethernet0/4  C>\* 192.168.10.0/24 is directly connected, ethernet0/1  H>\* 192.168.10.1/32 [0/0/1] is local address, ethernet0/1  C>\* 192.168.11.0/24 is directly connected, ethernet0/2  H>\* 192.168.11.1/32 [0/0/1] is local address, ethernet0/2  C>\* 192.168.121.0/24 is directly connected, ethernet0/0  H>\* 192.168.121.129/32 [0/0/1] is local address, ethernet0/0  C>\* 200.1.1.0/24 is directly connected, ethernet0/4  H>\* 200.1.1.1/32 [0/0/1] is local address, ethernet0/4  ==============================================================================  FW1# show snat  -------------------------------------------------------------------------------------------------------------------------------------  vr name:trust-vr  snat rules total number is :2  =====================================================================================================================================  id ingress if from to service egress if/vr translate to mode start end size  -------------------------------------------------------------------------------------------------------------------------------------  1 192.168.0.0/16 Any Any ethernet0/4 egress if's IP Dyn-Pt  2 192.168.0.0/16 Any Any ethernet0/4 egress if's IP Dyn-Pt  =====================================================================================================================================  FW1# conf  FW1# configure  FW1(config)# poli  FW1(config)# policy-gl  FW1(config)# policy-global  FW1(config-policy)# rule from any to any s  FW1(config-policy)# rule from any to any service any  application The application  deny Deny the traffic  fromtunnel Only traffic from this tunnel is permitted  permit Permit the traffic  portal-server Portal-server  tunnel Put the traffic to tunnel  webauth Webauth  FW1(config-policy)# rule from any to any service any per  FW1(config-policy)# rule from any to any service any permit  Rule id 2 is created  2022-05-12 07:14:26, Event CRIT@SECURITY: The user "hillstone" created a policy (id 2)  2022-05-12 07:14:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "action" has been set: "PERMIT"  2022-05-12 07:14:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "src-addr" has been added: Any  FW1(config-policy)# 2022-05-12 07:14:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "dst-addr" has been added: Any  2022-05-12 07:14:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "service" has been added: Any  FW1(config-policy)# end  FW1# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: n  Building configuration.2022-05-12 07:14:34, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  # 防火墙FW2配置  SG-6000# conf  SG-6000# configure  SG-6000(config)# hos  SG-6000(config)# hostn  SG-6000(config)# hostname FW2  2022-05-12 06:53:42, Event WARNING@MGMT: FW2(config)# Hostname is changed to FW2  FW2(config)# int  FW2(config)# interface e0/4  FW2(config-if-eth0/4)# zone u  FW2(config-if-eth0/4)# zone untrust  FW2(config-if-eth0/4)# ip add 100.0.0.1/24  2022-05-12 06:54:17, Event WARNING@NET: FW2(config-if-eth0/4)# interface ethernet0/4 turn to protocol up  2022-05-12 06:54:17, Event WARNING@NET: WAN interface IP address changes to 100.0.0.1  exi  FW2(config)# interface e0/4  FW2(config-if-eth0/4)# mana  FW2(config-if-eth0/4)# manage ping  FW2(config)# interface e0/1  FW2(config-if-eth0/1)# zone tr  FW2(config-if-eth0/1)# zone trust  FW2(config-if-eth0/1)# ip add 192.168.20.1/24  2022-05-12 07:20:59, Event WARNING@NET: FW2(config-if-eth0/1)# interface ethernet0/1 turn to protocol up  mana  FW2(config-if-eth0/1)# manage ping  FW2(config-if-eth0/1)# exi  FW2(config)# ip vr  FW2(config)# ip vrouter tr  FW2(config)# ip vrouter trust-vr  FW2(config-vrouter)# ip rout  FW2(config-vrouter)# ip route 0.0.0.0/0 100.0.0.254  2022-05-12 07:21:44, Network INFO@NET: FW2(config-vrouter)# Route in VR trust-vr that has IP address 0.0.0.0/0 through nexthop 100.0.0.254 with precedence 1 is created  FW2(config-vrouter)# sna  FW2(config-vrouter)# snatrule from 192.168.20.0/24 to any ser  FW2(config-vrouter)# snatrule from 192.168.20.0/24 to any service any eif  FW2(config-vrouter)# snatrule from 192.168.20.0/24 to any service any eif e0/4 tra  FW2(config-vrouter)# snatrule from 192.168.20.0/24 to any service any eif e0/4 trans-to ei  FW2(config-vrouter)# snatrule from 192.168.20.0/24 to any service any eif e0/4 trans-to eif-ip mod  FW2(config-vrouter)# snatrule from 192.168.20.0/24 to any service any eif e0/4 trans-to eif-ip mode d  rule ID=1  FW2(config-vrouter)# exi  FW2(config)# po  FW2(config)# policy-gl  FW2(config)# policy-global  FW2(config-policy)# ru  FW2(config-policy)# rule from any to any ser  FW2(config-policy)# rule from any to any service a  FW2(config-policy)# rule from any to any service any pe  FW2(config-policy)# rule from any to any service any permit  2022-05-12 07:22:49, Event CRIT@SECURITY: Rule id 1 is created  The user "hillstone" created a policy (id 1)  2022-05-12 07:22:49, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "action" has been set: "PERMIT"  2022-05-12 07:22:49, Event CRIT@SECURITY: FW2(config-policy)# The user "hillstone" modified the policy (id 1), the "src-addr" has been added: Any  2022-05-12 07:22:49, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "dst-addr" has been added: Any  2022-05-12 07:22:49, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "service" has been added: Any  FW2(config-policy)# exi  FW2(config)# show ip rou  FW2(config)# show ip route  Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,  B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, V - VPN, M - IMPORT,  I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, \* - FIB route, b - BFD enable  Routing Table for Virtual Router <trust-vr>  ==============================================================================  S>\* 0.0.0.0/0 [1/0/1] via 100.0.0.254, ethernet0/4  C>\* 100.0.0.0/24 is directly connected, ethernet0/4  H>\* 100.0.0.1/32 [0/0/1] is local address, ethernet0/4  C>\* 192.168.20.0/24 is directly connected, ethernet0/1  H>\* 192.168.20.1/32 [0/0/1] is local address, ethernet0/1  C>\* 192.168.121.0/24 is directly connected, ethernet0/0  H>\* 192.168.121.131/32 [0/0/1] is local address, ethernet0/0  ==============================================================================  # 防火墙FW3配置  login: hillstone  password:  SG-6000# con  SG-6000# configure  SG-6000(config)# host  host-blacklist Configure Host blacklist  host-book Configure host book  hostname Configure host name of the system  SG-6000(config)# hostn  SG-6000(config)# hostname FW3  2022-05-12 07:26:16, Event WARNING@MGMT: FW3(config)# Hostname is changed to FW3  inter  FW3(config)# interface e0/4  FW3(config-if-eth0/4)# zone tr  FW3(config-if-eth0/4)# zone un  FW3(config-if-eth0/4)# zone untrust  FW3(config-if-eth0/4)# zone tru  FW3(config-if-eth0/4)# zone trust  FW3(config-if-eth0/4)# zone un  FW3(config-if-eth0/4)# zone untrust  FW3(config-if-eth0/4)# ip add 101.0.0.1/24  2022-05-12 07:27:01, Event WARNING@NET: interface ethernet0/4 turn to protocol up  FW3(config-if-eth0/4)# 2022-05-12 07:27:01, Event WARNING@NET: WAN interface IP address changes to 101.0.0.1  FW3(config-if-eth0/4)# mana  FW3(config-if-eth0/4)# manage ping  FW3(config-if-eth0/4)# ping 101.0.0.254  Sending ICMP packets to 101.0.0.254  Seq ttl time(ms)  1 64 21.4  2 64 5.79  3 64 7.10  4 64 9.43  5 64 8.77  statistics:  5 packets sent, 5 received, 0% packet loss, time 4008ms  rtt min/avg/max/mdev = 5.798/10.506/21.418/5.603 ms  FW3(config-if-eth0/4)# inter  FW3(config-if-eth0/4)# interface e0/1  FW3(config-if-eth0/1)# zone  FW3(config-if-eth0/1)# zone tr  FW3(config-if-eth0/1)# zone trust  FW3(config-if-eth0/1)# ip ad  FW3(config-if-eth0/1)# ip address 192.168.30.1/24  2022-05-12 07:27:31, Event WARNING@NET: interface ethernet0/1 turn to protocol up  FW3(config-if-eth0/1)# man  FW3(config-if-eth0/1)# manage ping  <cr>  FW3(config-if-eth0/1)# manage ping  FW3(config-if-eth0/1)# exi  FW3(config)# ip vr  FW3(config)# ip vrouter  ^-----incomplete command  FW3(config)# ip vrouter tr  FW3(config)# ip vrouter trust-vr  FW3(config-vrouter)# ip route 0.0.0.0/0 101.0.0.254  2022-05-12 07:28:11, Network INFO@NET: FW3(config-vrouter)# Route in VR trust-vr that has IP address 0.0.0.0/0 through nexthop 101.0.0.254 with precedence 1 is created  FW3(config-vrouter)# sna  FW3(config-vrouter)# snatrule fro  FW3(config-vrouter)# snatrule from 192.168.30.0/24 to any ser  FW3(config-vrouter)# snatrule from 192.168.30.0/24 to any service any eif e0/4 tr  FW3(config-vrouter)# snatrule from 192.168.30.0/24 to any service any eif e0/4 trans-to e  FW3(config-vrouter)# snatrule from 192.168.30.0/24 to any service any eif e0/4 trans-to eif-ip m  FW3(config-vrouter)# snatrule from 192.168.30.0/24 to any service any eif e0/4 trans-to eif-ip mode d  FW3(config-vrouter)# snatrule from 192.168.30.0/24 to any service any eif e0/4 trans-to eif-ip mode dynamicport  rule ID=1  FW3(config-vrouter)# exi  FW3(config)# po  FW3(config)# policy-gl  FW3(config)# policy-global  FW3(config-policy)# rule from a  FW3(config-policy)# rule from any to  FW3(config-policy)# rule from any to a  FW3(config-policy)# rule from any to any s  FW3(config-policy)# rule from any to any service a  FW3(config-policy)# rule from any to any service an  FW3(config-policy)# rule from any to any service any per  FW3(config-policy)# rule from any to any service any permit  2022-05-12 07:29:23, Event CRIT@SECURITY: Rule id 1 is created  The user "hillstone" created a policy (id 1)  2022-05-12 07:29:23, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "action" has been set: "PERMIT"  FW3(config-policy)# 2022-05-12 07:29:23, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "src-addr" has been added: Any  2022-05-12 07:29:23, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "dst-addr" has been added: Any  2022-05-12 07:29:23, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 1), the "service" has been added: Any  FW3(config-policy)# end  FW3# show ip rou  FW3# show ip route  Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,  B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, V - VPN, M - IMPORT,  I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, \* - FIB route, b - BFD enable  Routing Table for Virtual Router <trust-vr>  ==============================================================================  S>\* 0.0.0.0/0 [1/0/1] via 101.0.0.254, ethernet0/4  C>\* 101.0.0.0/24 is directly connected, ethernet0/4  H>\* 101.0.0.1/32 [0/0/1] is local address, ethernet0/4  C>\* 192.168.30.0/24 is directly connected, ethernet0/1  H>\* 192.168.30.1/32 [0/0/1] is local address, ethernet0/1  C>\* 192.168.121.0/24 is directly connected, ethernet0/0  H>\* 192.168.121.130/32 [0/0/1] is local address, ethernet0/0  ==============================================================================  FW3# show snat  -------------------------------------------------------------------------------------------------------------------------------------  vr name:trust-vr  snat rules total number is :1  =====================================================================================================================================  id ingress if from to service egress if/vr translate to mode start end size  -------------------------------------------------------------------------------------------------------------------------------------  1 192.168.30.0/24 Any Any ethernet0/4 egress if's IP Dyn-Pt  =====================================================================================================================================  FW3# save  Save configuration, are you sure? [y]/n: y  Building configuration.2022-05-12 07:30:07, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW3# |

步骤二：完成IPSEC VPN路由配置；

|  |
| --- |
| # 防火墙FW1配置  FW1# conf  FW1(config)# ping 100.0.0.1  Sending ICMP packets to 100.0.0.1  Seq ttl time(ms)  1 127 17.0  2 127 11.2  3 127 13.6  4 127 12.4  5 127 18.1  statistics:  5 packets sent, 5 received, 0% packet loss, time 4004ms  rtt min/avg/max/mdev = 11.225/14.506/18.129/2.656 ms  FW1(config)# isak  FW1(config)# isakmp pe  FW1(config)# isakmp peer to-fw2  FW1(config-isakmp-peer)# int  FW1(config-isakmp-peer)# interface e0/4  FW1(config-isakmp-peer)# type sta  FW1(config-isakmp-peer)# type static  FW1(config-isakmp-peer)# mod  FW1(config-isakmp-peer)# mode ma  FW1(config-isakmp-peer)# mode main  FW1(config-isakmp-peer)# peer 100.0.0.1  FW1(config-isakmp-peer)# isk  FW1(config-isakmp-peer)# iskam  FW1(config-isakmp-peer)# iskam-p  FW1(config-isakmp-peer)# iskam-pro  FW1(config-isakmp-peer)# isakmp-  FW1(config-isakmp-peer)# isakmp-proposal ps  FW1(config-isakmp-peer)# isakmp-proposal psk-sha  FW1(config-isakmp-peer)# isakmp-proposal psk-sha256-aes  psk-sha256-aes128-g2  psk-sha256-aes256-g2  FW1(config-isakmp-peer)# isakmp-proposal psk-sha256-aes1  FW1(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW1(config-isakmp-peer)# pre-s  FW1(config-isakmp-peer)# pre-share 123456  FW1(config-isakmp-peer)# exi  FW1(config)# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: n  Building configuration.2022-05-12 07:40:04, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW1(config)# tunne  FW1(config)# tunnel ipsec  ^-----incomplete command  FW1(config)# tunnel ipsec ti  FW1(config)# tunnel ipsec to  FW1(config)# tunnel ipsec to-fw2 a  FW1(config)# tunnel ipsec to-fw2 auto  FW1(config-tunnel-ipsec-auto)# show tu  FW1(config-tunnel-ipsec-auto)# show tunnel ipse  FW1(config-tunnel-ipsec-auto)# show tunnel ipsec aut  FW1(config-tunnel-ipsec-auto)# show tunnel ipsec auto to-fw2  Name: to-fw2  scpu: auto  mode: tunnel  gateway:  proposal:  phase2 id: local 0.0.0.0/0 remote 0.0.0.0/0 service any  anti\_replay: 0  df\_bit: copy  idle-time: 0  set-commit-bit: disabled  auto connect: disabled  interface:  DHCP start interface  tunnel interface:  split-tunnel-routes:  vpn-track: disabled  Description:  Check-id: disabled  Dialup-control-id: disabled  FW1(config-tunnel-ipsec-auto)# isa  FW1(config-tunnel-ipsec-auto)# isakmp-peer to-fw2  FW1(config-tunnel-ipsec-auto)# ipse  FW1(config-tunnel-ipsec-auto)# ipsec-proposal  esp-sha256-aes128-g2  esp-sha256-aes128-g0  esp-sha256-aes256-g2  esp-sha256-aes256-g0  esp-sha256-3des-g2  esp-sha256-3des-g0  esp-md5-aes128-g2  esp-md5-aes128-g0  esp-md5-aes256-g2  esp-md5-aes256-g0  esp-md5-3des-g2  esp-md5-3des-g0  WORD Ipsec proposal one name  FW1(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW1(config-tunnel-ipsec-auto)# exi  FW1(config)# tunn  FW1(config)# tunnel ipsec to  FW1(config)# tunnel ipsec to-fw2 auto  FW1(config-tunnel-ipsec-auto)# auto-c  FW1(config-tunnel-ipsec-auto)# auto-connect  FW1(config-tunnel-ipsec-auto)# exi  FW1(config)# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: n  Building configuration.2022-05-12 07:42:22, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW1(config)# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: y  Building configuration.2022-05-12 07:42:28, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW1(config)# show tu  FW1(config)# show tunnel ips  FW1(config)# show tunnel ipsec auto to  FW1(config)# show tunnel ipsec auto to-fw2  Name: to-fw2  scpu: auto  mode: tunnel  gateway: to-fw2  proposal: esp-sha256-aes128-g2  phase2 id: local 0.0.0.0/0 remote 0.0.0.0/0 service any  anti\_replay: 0  df\_bit: copy  idle-time: 0  set-commit-bit: disabled  auto connect: enabled  interface: ethernet0/4  DHCP start interface  tunnel interface:  split-tunnel-routes:  vpn-track: disabled  Description:  Check-id: disabled  Dialup-control-id: disabled  FW1(config)#  # 防火墙FW2配置  login: hillstone  password:  FW2# conf  FW2(config)# isa  FW2(config)# isakmp p  peer Set isakmp peer name  proposal Set isakmp proposal name  FW2(config)# isakmp peer  WORD (length: 1-31) Isakmp peer name  FW2(config)# isakmp peer to-fw1  FW2(config-isakmp-peer)# int  FW2(config-isakmp-peer)# interface e0/4  FW2(config-isakmp-peer)# type sta  FW2(config-isakmp-peer)# type static  FW2(config-isakmp-peer)# mode main  FW2(config-isakmp-peer)# peer 200.1.1.1  FW2(config-isakmp-peer)# isa  FW2(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW2(config-isakmp-peer)# pre-share 123456  FW2(config-isakmp-peer)# exi  FW2(config)# tunn  FW2(config)# tunnel ips  FW2(config)# tunnel ipsec to-fw1 auto  FW2(config-tunnel-ipsec-auto)# isa  FW2(config-tunnel-ipsec-auto)# isakmp-peer to-fw1  FW2(config-tunnel-ipsec-auto)# ipse  FW2(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW2(config-tunnel-ipsec-auto)# auto-co  FW2(config-tunnel-ipsec-auto)# auto-connect  FW2(config-tunnel-ipsec-auto)# exi  FW2(config)# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: n  Building configuration.2022-05-12 07:56:36, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW2(config)# 2022-05-12 07:56:39, Event WARNING@VPN: IPSec tunnel:to-fw1 connected  show isa  FW2(config)# show isakmp  peer Show ISAKMP peer  proposal Show ISAKMP proposal  sa Show ISAKMP sa  FW2(config)# show isakmp sa  Total: 1  ================================================================================  Cookies Gateway Port Algorithms Lifetime  --------------------------------------------------------------------------------  9ab336e552~ 200.1.1.1 500 pre-share sha256/aes 86379  ================================================================================  FW2(config)# show ipsec sa  Total: 1  S - Status, I - Inactive, A - Active;  ================================================================================  Id VPN Peer IP Port Algorithms SPI Life(s) S  --------------------------------------------------------------------------------  1 to-fw1 >200.1.1.1 500 esp:aes/sha256/- 3f14a46f 28767 A  1 to-fw1 <200.1.1.1 500 esp:aes/sha256/- 07ad1742 28767 A  ================================================================================  FW2(config)# |

步骤三：配置策略放行；

|  |
| --- |
| # 防火墙FW1配置  FW1# conf  FW1(config)# isa  FW1(config)# isakmp pee  FW1(config)# isakmp peer to-fw2  FW1(config-isakmp-peer)# int  FW1(config-isakmp-peer)# interface e0/4  FW1(config-isakmp-peer)# mode main  FW1(config-isakmp-peer)# type static  FW1(config-isakmp-peer)# peer 100.0.0.1  FW1(config-isakmp-peer)# isap  FW1(config-isakmp-peer)# isa  FW1(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW1(config-isakmp-peer)# pre-share 123456  FW1(config-isakmp-peer)# exi  FW1(config)# tunnel ip  FW1(config)# tunnel ipsec to-  FW1(config)# tunnel ipsec to-fw2 auto  FW1(config)# tunnel ipsec to-fw2 auto  FW1(config-tunnel-ipsec-auto)# isa  FW1(config-tunnel-ipsec-auto)# isakmp-peer to-fw2  FW1(config-tunnel-ipsec-auto)# ipsec-pre  FW1(config-tunnel-ipsec-auto)# ipsec-pr  FW1(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW1(config-tunnel-ipsec-auto)# exi  FW1(config)# 2022-05-12 09:28:49, Event WARNING@VPN: IPSec tunnel:to-fw2 connected  FW1(config)# inter  FW1(config)# interface tunnel1  FW1(config-if-tun2)# zone VP  FW1(config-if-tun2)# zone VPNHub  FW1(config-if-tun2)# tun  FW1(config-if-tun2)# tunnel ipse  FW1(config-if-tun2)# tunnel ipsec to-fw2  FW1(config-if-tun2)# exi  FW1(config)# ip vr  FW1(config)# ip vrouter tr  FW1(config)# ip vrouter trust-vr  FW1(config-vrouter)# ip rou  FW1(config-vrouter)# ip route 192.168.20.0/24 tun  FW1(config-vrouter)# ip route 192.168.20.0/24 tunnel1  FW1(config-vrouter)# exi  FW1# conf  FW1(config)# isa  FW1(config)# isakmp p  peer Set isakmp peer name  proposal Set isakmp proposal name  FW1(config)# isakmp pee  FW1(config)# isakmp peer to-fw3  FW1(config-isakmp-peer)# int  FW1(config-isakmp-peer)# interface e0/4  FW1(config-isakmp-peer)# mode main  FW1(config-isakmp-peer)# type static  FW1(config-isakmp-peer)# peer 101.0.0.1  FW1(config-isakmp-peer)# isap  FW1(config-isakmp-peer)# isa  FW1(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW1(config-isakmp-peer)# pre-share 123456  FW1(config-isakmp-peer)# exi  FW1(config)# tunnel ip  FW1(config)# tunnel ipsec to-  FW1(config)# tunnel ipsec to-fw3 auto  FW1(config)# tunnel ipsec to-fw3 auto  FW1(config-tunnel-ipsec-auto)# isa  FW1(config-tunnel-ipsec-auto)# isakmp-peer to-fw3  FW1(config-tunnel-ipsec-auto)# ipsec-pre  FW1(config-tunnel-ipsec-auto)# ipsec-pr  FW1(config-tunnel-ipsec-auto)# ipsec-proposal psk-sha256-aes128-g2  Error: IPSec proposal psk-sha256-aes128-g2 does not exist  FW1(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW1(config-tunnel-ipsec-auto)# exi  FW1(config)# 2022-05-12 09:38:49, Event WARNING@VPN: IPSec tunnel:to-fw3 connected  FW1(config)# show isa sa  Total: 2  ================================================================================  Cookies Gateway Port Algorithms Lifetime  --------------------------------------------------------------------------------  2e31785e70~ 101.0.0.1 500 pre-share sha256/aes 86296  9ab336e552~ 100.0.0.1 500 pre-share sha256/aes 80167  ================================================================================  FW1(config)# inter  FW1(config)# interface tunnel2  FW1(config-if-tun2)# zone VP  FW1(config-if-tun2)# zone VPNHub  FW1(config-if-tun2)# tun  FW1(config-if-tun2)# tunnel ipse  FW1(config-if-tun2)# tunnel ipsec to-fw3  FW1(config-if-tun2)# exi  FW1(config)# ip vr  FW1(config)# ip vrouter tr  FW1(config)# ip vrouter trust-vr  FW1(config-vrouter)# ip rou  FW1(config-vrouter)# ip route 192.168.30.0/24 tun  FW1(config-vrouter)# ip route 192.168.30.0/24 tunnel2  2022-05-12 09:41:11, Network INFO@NET: FW1(config-vrouter)# Route in VR trust-vr that has IP address 192.168.30.0/24 through nexthop tunnel2 with precedence 1 is created  FW1(config-vrouter)# exi  FW1(config)# po  FW1(config)# policy-gl  FW1(config)# policy-global  FW1(config-policy)# rule from any to any from-zone VPNHub to-zone VPNHub service any permit  2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" created a policy (id 5)  Rule id 5 is created  2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 5), the "action" has been set: "PERMIT"  2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 5), the "src-addr" has been added: Any  2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 5), the "dst-addr" has been added: Any  2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 5), the "src-zone" has been modified: Any->VPNHub  2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 5), the "dst-zone" has been modified: Any->VPNHub  FW1(config-policy)# 2022-05-12 09:57:26, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 5), the "service" has been added: Any  FW1(config-policy)# save Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: n  Building configuration.2022-05-12 09:41:15, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW1(config-vrouter)#  # 防火墙FW2配置  FW2# conf  FW2(config)# isa  FW2(config)# isakmp pe  FW2(config)# isakmp peer to-fw1  FW2(config-isakmp-peer)# inter  FW2(config-isakmp-peer)# interface e0/4  FW2(config-isakmp-peer)# peer 200.1.1.1  FW2(config-isakmp-peer)# isa  FW2(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW2(config-isakmp-peer)# pre-share 123456  FW2(config-isakmp-peer)# exi  FW2(config)# tun  FW2(config)# tunnel ips  FW2(config)# tunnel ipsec to-f  FW2(config)# tunnel ipsec to-fw1 auto  FW2(config-tunnel-ipsec-auto)# isa  FW2(config-tunnel-ipsec-auto)# isakmp-peer to-fw1  FW2(config-tunnel-ipsec-auto)# ipse  FW2(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW2(config-tunnel-ipsec-auto)# auto-c  FW2(config-tunnel-ipsec-auto)# auto-connect  FW2(config-tunnel-ipsec-auto)# exi  FW2(config)# inter  FW2(config)# interface tunnel1  FW2(config-if-tun1)# zone Vp  FW2(config-if-tun1)# zone VPn  FW2(config-if-tun1)# zone VPN  FW2(config-if-tun1)# zone VPNHub  FW2(config-if-tun1)# tun  FW2(config-if-tun1)# tunnel 2022-05-12 09:38:49, Event WARNING@VPN: IPSec tunnel:to-fw1 connected  ipse  FW2(config-if-tun1)# tunnel ipsec to-fw1  FW2(config-if-tun1)# exi  FW2(config)# ip vr  FW2(config)# ip vrouter tr  FW2(config)# ip vrouter trust-vr  FW2(config-vrouter)# ip route 192.168.10.0/24 tu  FW2(config-vrouter)# ip route 192.168.10.0/24 tunnel1  2022-05-12 09:39:15, Network INFO@NET: FW2(config-vrouter)# Route in VR trust-vr that has IP address 192.168.10.0/24 through nexthop tunnel1 with precedence 1 is created  exi  FW2(config)# pol  FW2(config)# policy-gl  FW2(config)# policy-global  FW2(config-policy)# rule from  any Any ipv4 address  A.B.C.D/M Source ip/mask  WORD (length: 1-95) Name of address book  FW2(config-policy)# rule from an  FW2(config-policy)# rule from any to any  FW2(config-policy)# rule from any to any from-zone Vp  FW2(config-policy)# rule from any to any from-zone VP  FW2(config-policy)# rule from any to any from-zone VPNHub to-  FW2(config-policy)# rule from any to any from-zone VPNHub to-zone tr  FW2(config-policy)# rule from any to any from-zone VPNHub to-zone trust ser  FW2(config-policy)# rule from any to any from-zone VPNHub to-zone trust service any per  FW2(config-policy)# rule from any to any from-zone VPNHub to-zone trust service any permit  2022-05-12 09:40:05, Event CRIT@SECURITY: Rule id 2 is created  The user "hillstone" created a policy (id 2)  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "action" has been set: "PERMIT"  FW2(config-policy)# 2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "src-addr" has been added: Any  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "dst-addr" has been added: Any  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "src-zone" has been modified: Any->VPNHub  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "dst-zone" has been modified: Any->trust  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "service" has been added: Any  FW2(config)# isa  FW2(config)# isakmp peer to-fw3  FW2(config-isakmp-peer)# int  FW2(config-isakmp-peer)# interface e0/4  FW2(config-isakmp-peer)# peer 101.0.0.1  FW2(config-isakmp-peer)# isa  FW2(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW2(config-isakmp-peer)# pre-sh  FW2(config-isakmp-peer)# pre-share 123456  FW2(config-isakmp-peer)# exi  FW2(config)# tunn  FW2(config)# tunnel ip  FW2(config)# tunnel ipsec to-fw3 auto  FW2(config-tunnel-ipsec-auto)# isak  FW2(config-tunnel-ipsec-auto)# isakmp-peer to-fw3  FW2(config-tunnel-ipsec-auto)# ips  FW2(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW2(config-tunnel-ipsec-auto)# aut  FW2(config-tunnel-ipsec-auto)# auto-c  FW2(config-tunnel-ipsec-auto)# auto-connect  FW2(config-tunnel-ipsec-auto)# exi  FW2(config)# ip vr  FW2(config)# ip vrouter tr  FW2(config)# ip vrouter trust-vr  FW2(config-vrouter)# ip route 192.168.30.0/24 tu  FW2(config-vrouter)# ip route 192.168.30.0/24 tunnel1  2022-05-12 09:55:53, Network INFO@NET: FW2(config-vrouter)# Route in VR trust-vr that has IP address 192.168.30.0/24 through nexthop tunnel1 with precedence 1 is created  FW2(config-vrouter)# exi  FW2(config)# pol  FW2(config)# policy-gl  FW2(config)# policy-global  FW2(config-policy)# rule from2022-05-12 09:56:22, Event WARNING@VPN: IPSec tunnel:to-fw3 connected  ^-----incomplete command  FW2(config-policy)# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: y  Building configuration.2022-05-12 09:56:42, Event CRIT@MGMT: hillstone save system configuration via Console.  .  Saving configuration is finished  FW2(config-policy)#  # 防火墙FW3配置  FW3#  FW3#  FW3# conf  FW3(config)# isa  FW3(config)# isakmp pe  FW3(config)# isakmp peer to-fw1  FW3(config-isakmp-peer)# inter  FW3(config-isakmp-peer)# interface e0/4  FW3(config-isakmp-peer)# peer 200.1.1.1  FW3(config-isakmp-peer)# isa  FW3(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW3(config-isakmp-peer)# pre-share 123456  FW3(config-isakmp-peer)# exi  FW3(config)# tun  FW3(config)# tunnel ips  FW3(config)# tunnel ipsec to-f  FW3(config)# tunnel ipsec to-fw1 auto  FW3(config-tunnel-ipsec-auto)# isa  FW3(config-tunnel-ipsec-auto)# isakmp-peer to-fw1  FW3(config-tunnel-ipsec-auto)# ipse  FW3(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW3(config-tunnel-ipsec-auto)# auto-c  FW3(config-tunnel-ipsec-auto)# auto-connect  FW3(config-tunnel-ipsec-auto)# exi  FW3(config)# show isp sa  ^-----unrecognized keyword sa  FW3(config)# show ipsec sa  Total: 1  S - Status, I - Inactive, A - Active;  ================================================================================  Id VPN Peer IP Port Algorithms SPI Life(s) S  --------------------------------------------------------------------------------  1 to-fw1 >200.1.1.1 500 -:/-/-/- - 0 I  1 to-fw1 <200.1.1.1 - -:/-/-/- - 0 I  ================================================================================  FW3(config)# inter  FW3(config)# interface tunnel1  FW3(config-if-tun1)# zone Vp  FW3(config-if-tun1)# zone VPn  FW3(config-if-tun1)# zone VPN  FW3(config-if-tun1)# zone VPNHub  FW3(config-if-tun1)# tun  FW3(config-if-tun1)# tunnel 2022-05-12 09:38:49, Event WARNING@VPN: IPSec tunnel:to-fw1 connected  ipse  FW3(config-if-tun1)# tunnel ipsec to-fw1  FW3(config-if-tun1)# eix  ^-----unrecognized keyword eix  FW3(config-if-tun1)# exi  FW3(config)# ip vr  FW3(config)# ip vrouter tr  FW3(config)# ip vrouter trust-vr  FW3(config-vrouter)# ip route 192.168.10.0/24 tu  FW3(config-vrouter)# ip route 192.168.10.0/24 tunnel1  2022-05-12 09:39:15, Network INFO@NET: FW3(config-vrouter)# Route in VR trust-vr that has IP address 192.168.10.0/24 through nexthop tunnel1 with precedence 1 is created  exi  FW3(config)# pol  FW3(config)# policy-gl  FW3(config)# policy-global  FW3(config-policy)# rule from  any Any ipv4 address  A.B.C.D/M Source ip/mask  WORD (length: 1-95) Name of address book  FW3(config-policy)# rule from an  FW3(config-policy)# rule from any to any  FW3(config-policy)# rule from any to any from-zone Vp  FW3(config-policy)# rule from any to any from-zone VP  FW3(config-policy)# rule from any to any from-zone VPNHub to-  FW3(config-policy)# rule from any to any from-zone VPNHub to-zone tr  FW3(config-policy)# rule from any to any from-zone VPNHub to-zone trust ser  FW3(config-policy)# rule from any to any from-zone VPNHub to-zone trust service any per  FW3(config-policy)# rule from any to any from-zone VPNHub to-zone trust service any permit  2022-05-12 09:40:05, Event CRIT@SECURITY: Rule id 2 is created  The user "hillstone" created a policy (id 2)  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "action" has been set: "PERMIT"  FW3(config-policy)# 2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "src-addr" has been added: Any  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "dst-addr" has been added: Any  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "src-zone" has been modified: Any->VPNHub  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "dst-zone" has been modified: Any->trust  2022-05-12 09:40:05, Event CRIT@SECURITY: The user "hillstone" modified the policy (id 2), the "service" has been added: Any  FW3(config-policy)#  FW3(config-policy)# isa  FW3(config-policy)# isa  FW3(config-policy)# exi  FW3(config)# isa  FW3(config)# isakmp pee  FW3(config)# isakmp peer to-fw2  FW3(config-isakmp-peer)# int  FW3(config-isakmp-peer)# interface e0/4  FW3(config-isakmp-peer)# mode main  FW3(config-isakmp-peer)# type static  FW3(config-isakmp-peer)# peer 100.0.0.1  FW3(config-isakmp-peer)# isa  FW3(config-isakmp-peer)# isakmp-proposal psk-sha256-aes128-g2  FW3(config-isakmp-peer)# pre-share 123456  FW3(config-isakmp-peer)# exi  FW3(config)# tunn  FW3(config)# tunnel ip  FW3(config)# tunnel ipsec to-fw2 auto  FW3(config-tunnel-ipsec-auto)# isa  FW3(config-tunnel-ipsec-auto)# isakmp-peer to-fw2  FW3(config-tunnel-ipsec-auto)# isp  FW3(config-tunnel-ipsec-auto)# ipse  FW3(config-tunnel-ipsec-auto)# ipsec-proposal esp-sha256-aes128-g2  FW3(config-tunnel-ipsec-auto)# exi  FW3(config)# ip vr  FW3(config)# ip vrouter tru  FW3(config)# ip vrouter trust-vr  FW3(config-vrouter)# ip route 192.168.20.0/24 tun  FW3(config-vrouter)# ip route 192.168.20.0/24 tunnel1  2022-05-12 09:52:53, Network INFO@NET: FW3(config-vrouter)# Route in VR trust-vr that has IP address 192.168.20.0/24 through nexthop tunnel1 with precedence 1 is created  FW3(config-vrouter)# save  Save configuration, are you sure? [y]/n: y  Backup start configuration file, are you sure? y/[n]: y  Building configuration.2022-05-12 09:52:59, Event CRIT@MGMT: hillstone save system configuration via Console.  Saving configuration is finished |

1. 实验结果

/\*\*\*分点描述具体实验现象 \*\*\*/

1. VPC4：

VPCS> ip 192.168.10.10 255.255.255.0 192.168.10.1

Checking for duplicate address...

PC1 : 192.168.10.10 255.255.255.0 gateway 192.168.10.1

VPCS> ping 200.1.1.254

200.1.1.254 icmp\_seq=1 timeout

200.1.1.254 icmp\_seq=2 timeout

200.1.1.254 icmp\_seq=3 timeout

200.1.1.254 icmp\_seq=4 timeout

ping 200.1.1.254 icmp\_seq=5 timeout

100

VPCS> ping 100.0.0.254

100.0.0.254 icmp\_seq=1 timeout

100.0.0.254 icmp\_seq=2 timeout

100.0.0.254 icmp\_seq=3 timeout

100.0.0.254 icmp\_seq=4 timeout

100.0.0.254 icmp\_seq=5 timeout

VPCS> ping 192.168.20.20

192.168.20.20 icmp\_seq=1 timeout

84 bytes from 192.168.20.20 icmp\_seq=2 ttl=62 time=16.322 ms

84 bytes from 192.168.20.20 icmp\_seq=3 ttl=62 time=16.589 ms

84 bytes from 192.168.20.20 icmp\_seq=4 ttl=62 time=18.303 ms

84 bytes from 192.168.20.20 icmp\_seq=5 ttl=62 time=25.515 ms

VPCS> ping 192.168.30.30

84 bytes from 192.168.30.30 icmp\_seq=1 ttl=62 time=32.783 ms

84 bytes from 192.168.30.30 icmp\_seq=2 ttl=62 time=14.355 ms

84 bytes from 192.168.30.30 icmp\_seq=3 ttl=62 time=16.276 ms

84 bytes from 192.168.30.30 icmp\_seq=4 ttl=62 time=14.286 ms

84 bytes from 192.168.30.30 icmp\_seq=5 ttl=62 time=17.364 ms

VPCS> ping 192.168.11.11

84 bytes from 192.168.11.11 icmp\_seq=1 ttl=63 time=1.935 ms

84 bytes from 192.168.11.11 icmp\_seq=2 ttl=63 time=0.877 ms

84 bytes from 192.168.11.11 icmp\_seq=3 ttl=63 time=0.663 ms

84 bytes from 192.168.11.11 icmp\_seq=4 ttl=63 time=1.068 ms

84 bytes from 192.168.11.11 icmp\_seq=5 ttl=63 time=1.435 ms

1. VPC7

VPCS> ip 192.168.20.20/24 192.168.20.1

Checking for duplicate address...

PC1 : 192.168.20.20 255.255.255.0 gateway 192.168.20.1

VPCS> ping 192.168.20.1

ping 100.^Hhost (192.168.20.1) not reachable

VPCS> ping 192.168.20.1

192.168.20.1 icmp\_seq=1 timeout

84 bytes from 192.168.20.1 icmp\_seq=2 ttl=128 time=1.150 ms

84 bytes from 192.168.20.1 icmp\_seq=3 ttl=128 time=1.302 ms

84 bytes from 192.168.20.1 icmp\_seq=4 ttl=128 time=1.311 ms

84 bytes from 192.168.20.1 icmp\_seq=5 ttl=128 time=1.147 ms

VPCS> ping 100.0.0.254

84 bytes from 100.0.0.254 icmp\_seq=1 ttl=63 time=19.896 ms

ping 2084 bytes from 100.0.0.254 icmp\_seq=2 ttl=63 time=13.263 ms

0.1.184 bytes from 100.0.0.254 icmp\_seq=3 ttl=63 time=7.626 ms

.2584 bytes from 100.0.0.254 icmp\_seq=4 ttl=63 time=9.027 ms

484 bytes from 100.0.0.254 icmp\_seq=5 ttl=63 time=7.268 ms

VPCS> ping 200.1.1.254

84 bytes from 200.1.1.254 icmp\_seq=1 ttl=63 time=10.744 ms

84 bytes from 200.1.1.254 icmp\_seq=2 ttl=63 time=6.574 ms

84 bytes from 200.1.1.254 icmp\_seq=3 ttl=63 time=23.901 ms

84 bytes from 200.1.1.254 icmp\_seq=4 ttl=63 time=13.179 ms

84 bytes from 200.1.1.254 icmp\_seq=5 ttl=63 time=9.476 ms

VPCS> ping 192.168.10.10

84 bytes from 192.168.10.10 icmp\_seq=1 ttl=62 time=16.776 ms

84 bytes from 192.168.10.10 icmp\_seq=2 ttl=62 time=13.731 ms

84 bytes from 192.168.10.10 icmp\_seq=3 ttl=62 time=19.043 ms

84 bytes from 192.168.10.10 icmp\_seq=4 ttl=62 time=43.834 ms

84 bytes from 192.168.10.10 icmp\_seq=5 ttl=62 time=55.373 ms

VPCS> ping 192.168.11.11

\*100.0.0.254 icmp\_seq=1 ttl=63 time=12.512 ms (ICMP type:3, code:0, Destination network unreachable)

\*100.0.0.254 icmp\_seq=2 ttl=63 time=6.654 ms (ICMP type:3, code:0, Destination network unreachable)

\*100.0.0.254 icmp\_seq=3 ttl=63 time=12.958 ms (ICMP type:3, code:0, Destination network unreachable)

\*100.0.0.254 icmp\_seq=4 ttl=63 time=9.118 ms (ICMP type:3, code:0, Destination network unreachable)

\*100.0.0.254 icmp\_seq=5 ttl=63 time=13.329 ms (ICMP type:3, code:0, Destination network unreachable)

VPCS> ping 192.168.30.30

84 bytes from 192.168.30.30 icmp\_seq=1 ttl=61 time=51.029 ms

84 bytes from 192.168.30.30 icmp\_seq=2 ttl=61 time=33.734 ms

84 bytes from 192.168.30.30 icmp\_seq=3 ttl=61 time=37.673 ms

84 bytes from 192.168.30.30 icmp\_seq=4 ttl=61 time=35.739 ms

84 bytes from 192.168.30.30 icmp\_seq=5 ttl=61 time=37.642 ms

1. VPC8

VPCS> ip 192.168.30.30/24 192.168.30.1

Checking for duplicate address...

ping PC1 : 192.168.30.30 255.255.255.0 gateway 192.168.30.1

VPCS> ping 192.168.30.1

ping 101192.168.30.1 icmp\_seq=1 timeout

84 bytes from 192.168.30.1 icmp\_seq=2 ttl=128 time=0.569 ms

84 bytes from 192.168.30.1 icmp\_seq=3 ttl=128 time=0.852 ms

84 bytes from 192.168.30.1 icmp\_seq=4 ttl=128 time=0.590 ms

84 bytes from 192.168.30.1 icmp\_seq=5 ttl=128 time=0.578 ms

VPCS> ping 101.0.0.254

84 bytes from 101.0.0.254 icmp\_seq=1 ttl=63 time=14.937 ms

84 bytes from 101.0.0.254 icmp\_seq=2 ttl=63 time=7.218 ms

poin84 bytes from 101.0.0.254 icmp\_seq=3 ttl=63 time=6.132 ms

^H^H^H84 bytes from 101.0.0.254 icmp\_seq=4 ttl=63 time=6.090 ms

^H^H^H^H84 bytes from 101.0.0.254 icmp\_seq=5 ttl=63 time=6.494 ms

VPCS> ping 100.0.0.254

84 bytes from 100.0.0.254 icmp\_seq=1 ttl=63 time=12.176 ms

84 bytes from 100.0.0.254 icmp\_seq=2 ttl=63 time=9.938 ms

84 bytes from 100.0.0.254 icmp\_seq=3 ttl=63 time=6.624 ms

84 bytes from 100.0.0.254 icmp\_seq=4 ttl=63 time=11.051 ms

84 bytes from 100.0.0.254 icmp\_seq=5 ttl=63 time=10.523 ms

VPCS> ping 192.168.10.10

84 bytes from 192.168.10.10 icmp\_seq=1 ttl=62 time=32.937 ms

84 bytes from 192.168.10.10 icmp\_seq=2 ttl=62 time=13.125 ms

84 bytes from 192.168.10.10 icmp\_seq=3 ttl=62 time=12.128 ms

84 bytes from 192.168.10.10 icmp\_seq=4 ttl=62 time=15.257 ms

84 bytes from 192.168.10.10 icmp\_seq=5 ttl=62 time=12.218 ms

VPCS> ping 192.168.20.20

84 bytes from 192.168.20.20 icmp\_seq=1 ttl=61 time=37.318 ms

84 bytes from 192.168.20.20 icmp\_seq=2 ttl=61 time=35.057 ms

84 bytes from 192.168.20.20 icmp\_seq=3 ttl=61 time=32.120 ms

84 bytes from 192.168.20.20 icmp\_seq=4 ttl=61 time=33.757 ms

84 bytes from 192.168.20.20 icmp\_seq=5 ttl=61 time=62.417 ms

VPCS> ping 192.168.11.11

84 bytes from 192.168.11.11 icmp\_seq=1 ttl=63 time=1.935 ms

84 bytes from 192.168.11.11 icmp\_seq=2 ttl=63 time=0.877 ms

84 bytes from 192.168.11.11 icmp\_seq=3 ttl=63 time=0.663 ms

84 bytes from 192.168.11.11 icmp\_seq=4 ttl=63 time=1.068 ms

84 bytes from 192.168.11.11 icmp\_seq=5 ttl=63 time=1.435 ms

1. 总结分析

通过课程和实验的学习，我学到了在面对诸如企业在两地分别创建办公环境之类的问题时，为保证信息安全，打造安全的内网环境的方法，以及为了降低成本，采用在ISP提供的基础上使用VPN隧道服务，在公用的网络中创建专用的虚拟网络的技术。通过这次实验我学到了很多东西，不仅使我在理论上对网络有了全新的认识，在实践能力上也得到了提高，真正地做到了学以致用，更学到了很多做人的道理，对我来说受益非浅。