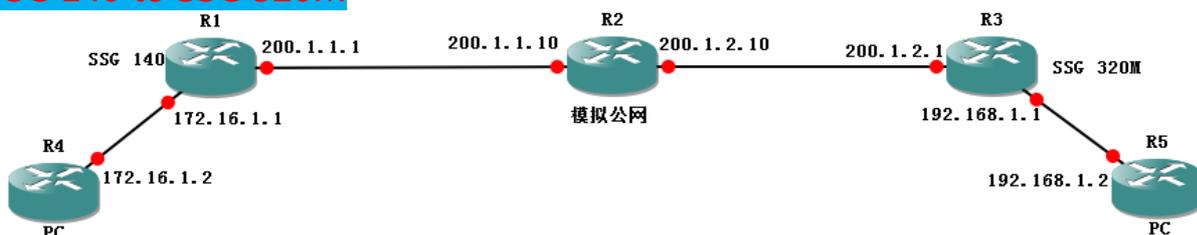


# LAN to LAN | SSG---SSG | 基于路由

## SSG 140 to SSG 320M



基于路由的方式：（以下是SSG140的配置，SSG320M的配置完全一致）

1、运营商的路由器有到达公网的路由，在此环境中，即R2只有直连路由即可。SSG140 模拟公司上网环境，写一条默认路由指向运营商，SSG 320M模拟公司上网环境，写一条默认路由指向运营商。

Network > Routing > Routing Entries SSG140

List 20 per page

List route entries for All virtual routers trust-vr New

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	172.16.1.0/24		ethernet0/0	C			Root		-
*	172.16.1.1/32		ethernet0/0	H			Root		-
*	200.1.1.0/24		ethernet0/2	C			Root		-
*	200.1.1.1/32		ethernet0/2	H			Root		-
*	0.0.0.0/0	200.1.1.10	ethernet0/2	SP	20	1	Root		Remove

\* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route  
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2  
 D Dynamic N NHRP

## 2、建立tunnel接口，

Network > Interfaces (List) SSG140

List 20 per page

List ALL(15) Interfaces

New Tunnel IF

Network > Interfaces > Edit SSG140

Interface: tunnel.1 (IP/Netmask: 0.0.0.0/0) Back To Interface List

Properties: Basic Proxy ARP MIP DIP VIP IGMP NHTB Tunnel IRDP

Tunnel Interface Name tunnel.1 指定tunnel接口的编号

Zone (VR) Trust (trust-vr) 指定tunnel接口属于的zone。此处若选择untrust，之后需要建立trust zone到untrust zone的policy。

Fixed IP

IP Address / Netmask 0.0.0.0 / 0

Unnumbered

Interface ethernet0/2 (trust-vr) tunnel接口绑定到防火墙出接口

Maximum Transfer Unit(MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy

Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps Guaranteed Bandwidth 0 Kbps Ingress Maximum Bandwidth 0 Kbps

NHRP Enable

ACVPN Dynamic Routing

Admin Status Up

## 3、第一阶段配置

Gateway Name  → 第一阶段的名字

Version  IKEv1  IKEv2

---

Remote Gateway

- Static IP Address IP Address/Hostname  → 对端的公网出口IP
- Dynamic IP Address Peer ID
- Dialup User User
- Dialup User Group Group

ACVPN-Dynamic Local ID

ACVPN-Profile

OK Cancel Advanced

点击Advanced ,

IKEv2 Auth Method

Self  Peer

---

Preshared Key   Use As Seed → 预共享密钥，两端必须相同

Local ID  (optional)

Outgoing Interface

---

Security Level

Predefined  Standard  Compatible  Basic

User Defined  Custom → 安全级别，两端必须一致

Phase 1 Proposal

Mode (Initiator)  Main (ID Protection)  Aggressive

---

Enable NAT-Traversal

UDP Checksum

Keepalive Frequency  Seconds (0~300)

---

Peer Status Detection

Heartbeat

Hello  Seconds (1~3600, 0: disable)

Reconnect  Seconds (60~9999, 0: default)

Threshold  (2-9999)

DPD

Interval  Seconds (3~28800, 0: disable)

Retry  (1~127)

Always Send

Reconnect Interval  (60~9999) Seconds, 0 Disable

## 4、第二阶段配置

VPN Name  → 第二阶段的名字

Remote Gateway

- Predefined  → 选择之前建立的第一阶段名字
- Create a Simple Gateway

Gateway Name

Version  IKEv1  IKEv2

Type  Static IP Address/Hostname

Dynamic IP Peer ID

Dialup User User

Dialup Group Group

Local ID  (optional)

Preshared Key   Use As Seed

Security Level  Standard  Compatible  Basic

Outgoing Interface

Gateway  Tunnel Towards Hub

Binding to Tunnel

OK Cancel Advanced

点击Advanced ,

**Security Level**

Predefined  Standard  Compatible  Basic  
 User Defined  Custom

**Phase 2 Proposal**  
 nopfs-esp-aes128-sha | None | None | None

Replay Protection   
 Transport Mode

Bind to  None  Tunnel Interface  Tunnel Zone  
 tunnel.1 | Untrust-Tun

Proxy-ID Check

DSCP Marking  Disable  Enable  
 Dscp Value 0

VPN Group None | Weight 0

VPN Monitor   
 Source Interface default  
 Destination IP default  
 Optimized   
 Rekey

Return Cancel

选择VPN绑定的 tunnel接口

5、写路由的方式匹配感兴趣流

Virtual Router Name trust-vr  
 IP Address/Netmask 192.168.1.0 / 24

Next Hop  Virtual Router untrust-vr  Gateway

Interface tunnel.1  
 Gateway IP Address 0.0.0.0  
 Permanent   
 Tag 0

Metric 1  
 Preference 20  
 Description

OK Cancel

用路由匹配感兴趣流

网关指向tunnel接口

List 20 per page

List route entries for All virtual routers

trust-vr New

trust-vr									
	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	172.16.1.0/24		ethernet0/0	C			Root		-
*	172.16.1.1/32		ethernet0/0	H			Root		-
*	200.1.1.0/24		ethernet0/2	C			Root		-
*	200.1.1.1/32		ethernet0/2	H			Root		-
*	0.0.0.0/0	200.1.1.10	ethernet0/2	SP	20	1	Root		<a href="#">Remove</a>
*	192.168.1.0/24		tunnel.1	S	20	1	Root		<a href="#">Remove</a>

\* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route  
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2  
 D Dynamic N NHRP

6、验证，建立成功：

List 20 per page

Show All Filter

VPN Name	SA ID	Policy ID	Peer Gateway IP	Type	SA Status	Link
to-SSG320-p2	00000003	-1/-1	200.1.2.1	AutoIKE	Active	Up

Date / Time	Level	Description
2015-04-01 13:09:01	info	IKE 200.1.2.1 Phase 2 msg ID 86d39e6b: Completed negotiations with SPI 3ac5788f, tunnel ID 3, and lifetime 3600 seconds/0 KB.
2015-04-01 13:09:01	info	IKE 200.1.2.1 phase 2:The symmetric crypto key has been generated successfully.
2015-04-01 13:09:01	info	IKE 200.1.2.1: Received a notification message for DOI 1 40001 NOTIFY_NS_NHTB_INFORM.
2015-04-01 13:09:01	info	IKE 200.1.2.1 Phase 2: Initiated negotiations.
2015-04-01 13:09:01	info	IKE 200.1.2.1 Phase 1: Completed Main mode negotiations with a 28800-second lifetime.
2015-04-01 13:09:01	info	IKE 200.1.2.1 phase 1:The symmetric crypto key has been generated successfully.
2015-04-01 13:09:01	info	IKE200.1.1.1 200.1.2.1 Phase 1: Initiated negotiations in main mode.

```
C:\Users\Zeus>ping 192.168.1.2 -t
正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间=1ms TTL=126
```

## 7、两端网段可以不匹配