Quick Setup IPSec VPN On Bivocom Router

**By Bivocom
Product Team**

1. Network Topology

R1

IP： 192.168.2.10

R2

R3

WAN：192.168.2.200

WAN: 192.168.2.100

LAN: 192.168.200.0/24
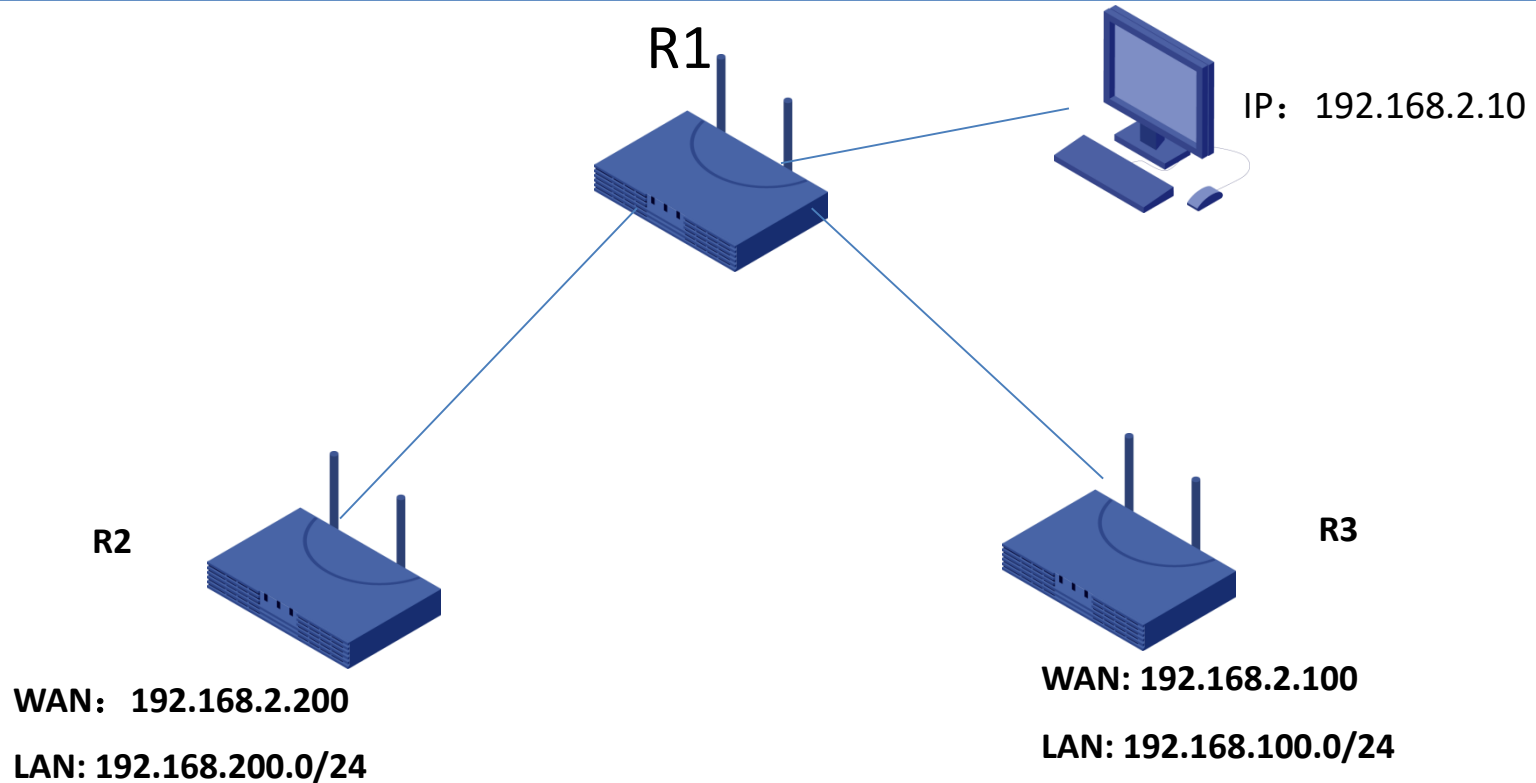
LAN: 192.168.100.0/24

Note:

1) R2 WAN port connect to R1 LAN to get a IP address 192.168.2.200; also R2 has its own LAN subnet 192.168.200.0/24;

2) R3 WAN port connect to R1 LAN to get a IP address 192.168.2.100; also R3 has its own LAN subnet 192.168.100.0/24;

3) **R2 LAN can't communicate with R3 LAN for each other, we need setup a VPN tunnel between R2 LAN and R3 LAN.**

2. Configure VPN Server

① **Configure R2 as a IPSec VPN Server via WebUI>>VPN>>IPSec.**

2. Configure VPN Server

② **Configure R2 as a IPSec VPN Server via WebUI>>VPN>>IPSec.**

IKE Life Time	28800
Authentication Type	Pre-shared Key
Pre-shared Key	123456abc
Local Identifier	222222222 → Set the local Identifier code.
Peer Identifier	111111111 → Input the Client/peer side Identifier code.
ESP Encryption Algorithm	AES-128
ESP Integrity Algorithm	SHA-1
DPD Timeout	60 seconds
DPD Detection Period	60 seconds
DPD Action	Restart

Save & Apply   Save   Reset

① **Configure R3 as a IPSec VPN Client via WebUI>>VPN>>IPSec.**

> View
> Setup
> Secure
∨ VPN
  PPTP
  L2TP
  IPSec
  OpenVPN
> Advanced
> Administrate
Logout

IPSec Connection Configuration

(VPN Client Side Settings)

IPSec Parameters

IPSec	⦿ Enable ◯ Disable
Peer Address	192.168.2.200	→ Input VPN Server address.
Negotiation Method	Main
Tunnel Type	Site To Site
Local Subnet	192.168.100.0/24	Set local subnet. ❓ eg: 192.168.10.0/24
Peer Subnet	192.168.200.0/24	Input Server side subnet ❓ eg: 192.168.20.0/24
IKE Encryption Algorithm	AES-128
IKE Integrity Algorithm	SHA-1
Diffie-Hellman Group	Group14(2048bits)

② **Configure R3 as a IPSec VPN Client via WebUI>>VPN>>IPSec.**

IKE Life Time	28800
Authentication Type	Pre-shared Key
Pre-shared Key	123456abc
Local Identifier	111111111
Peer Identifier	222222222
ESP Encryption Algorithm	AES-128
ESP Integrity Algorithm	SHA-1
DPD Timeout	60 seconds
DPD Detection Period	60 seconds
DPD Action	Restart

→ Set your local Identifier code.

→ Input Server side Identifier.

Save & Apply   Save   Reset

4. Check VPN Connection status on Client

① After configured VPN server and VPN client settings, check the VPN Client connection status via WebUI>>View>>VPN Status.

If everything goes well, the connect status would be CONNECTED.

5. Network Topology after setup VPN

R1

IP：192.168.2.10

R2

(VPN Server)

WAN：192.168.2.200

LAN: 192.168.200.0/24

R3

(VPN Client)

WAN: 192.168.2.100

LAN: 192.168.100.0/24
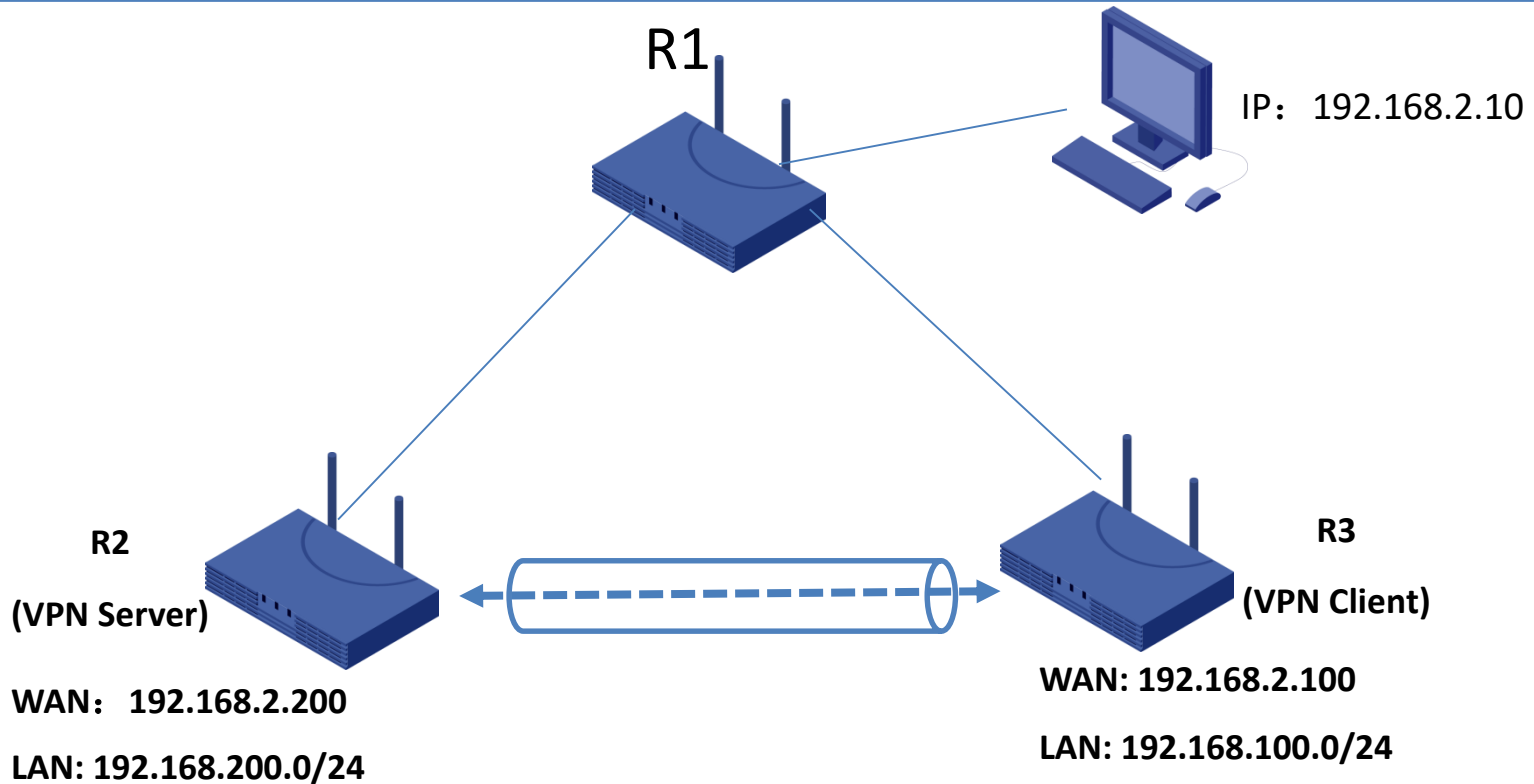
Note:

1) R2 as a VPN Server, the WAN port connect to R1 LAN to get a IP address 192.168.2.200; also R2 has its own LAN subnet 192.168.200.0/24;

2) R3 as a VPN Client, the WAN port connect to R1 LAN to get a IP address 192.168.2.100; also R3 has its own LAN subnet 192.168.100.0/24;

3) **After VPN configuration, R2 LAN with R3 LAN setup a VPN tunnel to communicate each other.**

Enjoy the Bivocom IPSec VPN feature ☺