LINKSYS RV082 VPN ROUTER
Interoperability Profile

Overview

This document describes how to configure Linksys RV082 VPN Router to implement Scenario 1 that the VPN Consortium specifies in "Documentation Profiles for IPSec Interoperability,"
http://www.vpnc.org/InteropProfiles/Interop-01.html
Scenario 1 is a gateway-to-gateway configuration with pre-shared secrets for authentication.

A Gateway-to-Gateway VPN Configuration

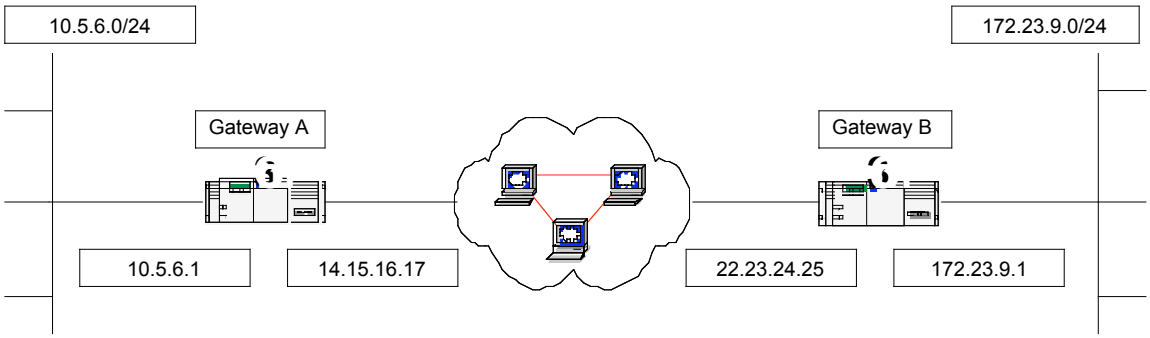


Figure 1 Gateway-to-Gateway VPN Configuration

• Gateway A (Linksys RV082) connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface IP address is 10.5.6.1, and its WAN interface IP address is 14.15.16.17

• Gateway B (VPNC devices) connects the internal LAN 172.23.9.0/24 to the Internet. Gateway A's LAN interface IP address is 172.23.9.1 and its WAN interface IP address is 22.23.24.25

The IKE Phase I parameters used in Scenario 1 are:
• Main mode
• Triple DES
• SHA-1
• MODP group 2 (1024 bits)
• Pre-shared secret of "hr5xb84l6aa9r6"
• SA lifetime of 28800 seconds (8 hours) with no kbytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:
• Triple DES
• SHA-1
• MODP group 2 (1024 bits)
• Perfect forward secrecy (PFS Enable) for rekeying
• SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
Traffic for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets.

Configuring RV082 VPN Router

Default LAN private address is http://192.168.1.1. Please connect your PC to RV082 LAN port and use the browser to control the RV082.

Setting up testing environment

You must use the HTML-based User Interface for the first configuration step to set up the system time and date, and configuring the private Ethernet interface (to the internal LAN), as described in the following steps. Then

Step 1 You started the RV082 VPN Router and use your browser to connect to RV082 system by connecting your PC to RV082 LAN port IP address http://192.168.1.1. (You may see a login/password popup screen as you successfully connect to RV082 VPN Router.

Step 2 At the popup screen, enter the default login name: **admin**. At the password prompt, enter the default password:

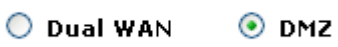
```
Login: admin
Password: admin
```

Step 3 The system displays the summary of the current status and you can set the time on Setup=>Time for RV082 VPN Router. The correct time is very important, so that logging and accounting entries are accurate. The time in brackets is the current device time.

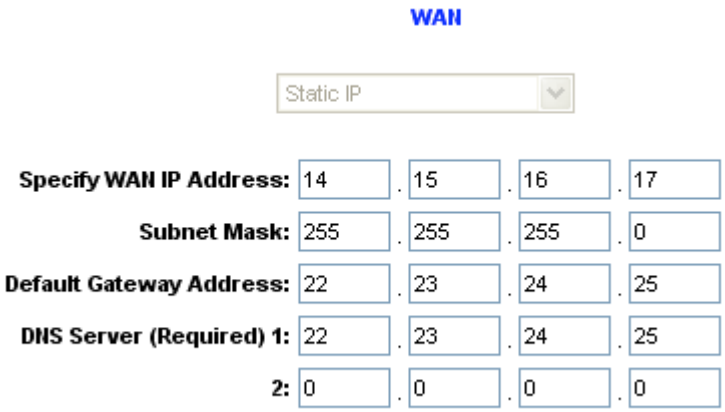
Step 4 You can setup the Private IP address at Setup=>Network. This is the Router's LAN IP Address and Subnet Mask. The default value is 192.168.1.1 for IP address and 255.255.255.0 for the Subnet Mask. Please enter the value as needed (Device IP Address = 10.5.6.1; Subnet Mask=255.255.255.0) and the system will be restarted automatically.

Step 5 Before choosing the following WAN Connection Type, please choose the Dual-WAN / DMZ Setting first at Setup=>Network. When DMZ selected, the WAN Connection Type will be limited as Static IP only, and DNS Server can't be setup either. Please select DMZ mode to simplify the IPSec testing environment.

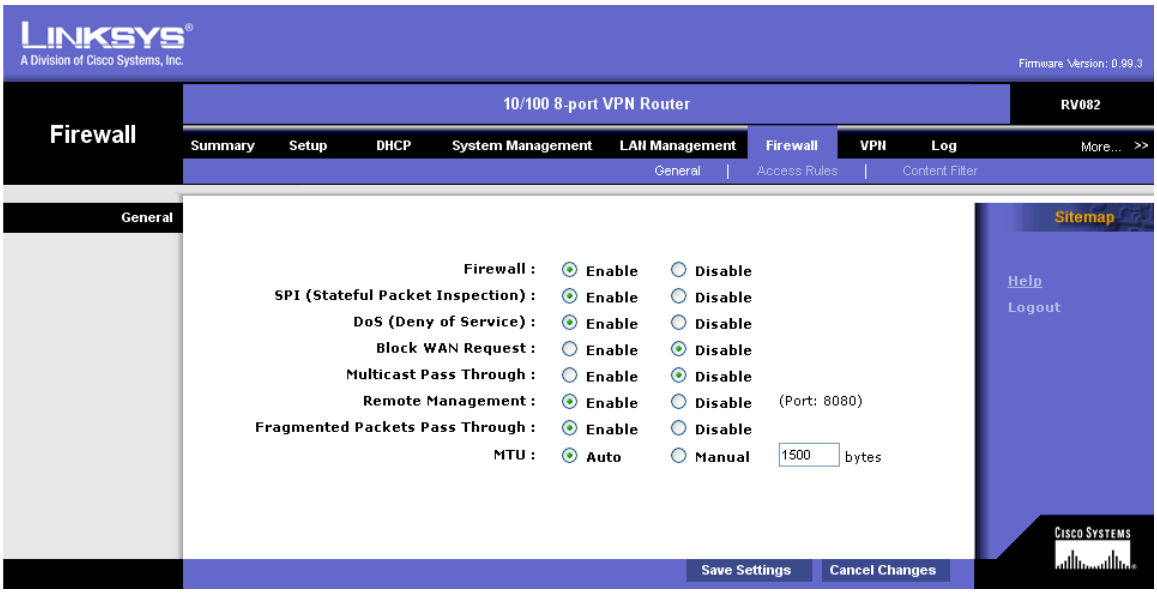
Dual-WAN / DMZ Setting



Step 6 In Setup=>Network, choose the WAN1 connection type as “Static IP” and setup the public IP address, Default gateway and DNS Server as needed (WAN IP Address=14.15.16.17; Subnet Mask=255.255.255.0; Default Gateway=22.23.24.25).



Step 7 In Firewall=>General, setup the firewall configuration as needed. Please Disable Block WAN Request and Enable Fragmented Packet Pass Through to let go of the IPSec Packets in RV082 VPN Router.



Overview of RV082 VPN IPSec tunnel Configuration

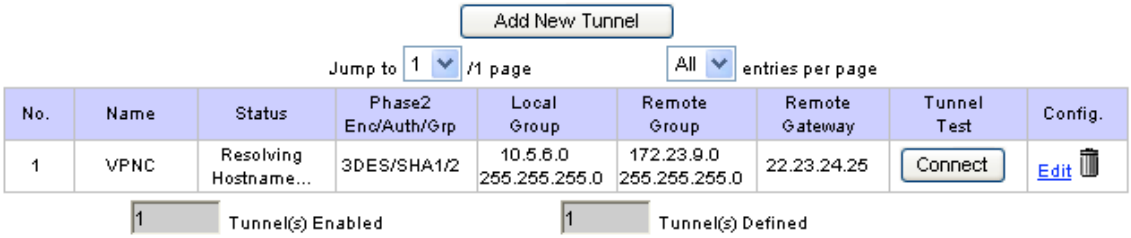
The VPN Summary displays the Summary, Tunnel Status and GroupVPN Status.

Summary:

It shows the amount of **Tunnel(s) Used** and **Tunnel(s) Available**. RV082 supports 1,000 tunnels.

Detail: Click the Detail button to see the detail of VPN Summary as below, and user can save and export the file.

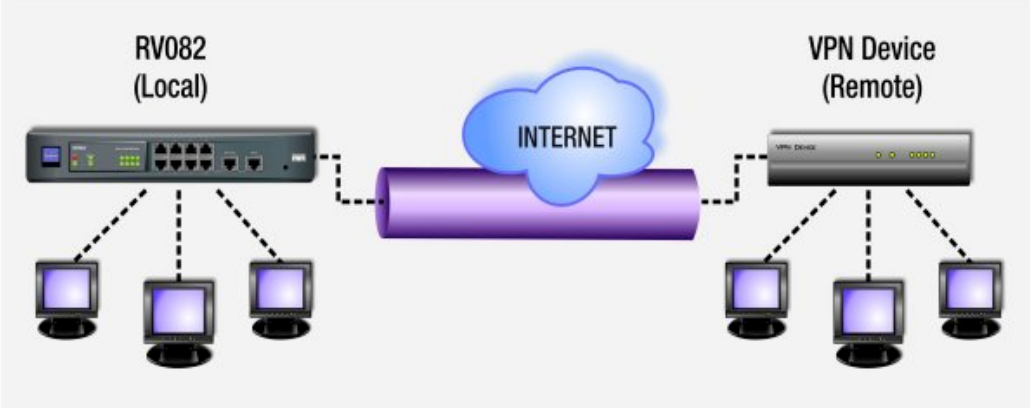
Tunnel Status:



Add New Tunnel:

Gateway to Gateway Tunnel:

The following figure illustrates the Gateway to Gateway tunnel. A tunnel created between two VPN Routers. When click “Add Now”, it will show **Add New Gateway to Gateway Tunnel** page.



Page: Previous page, Next page, Jump to page / 50 pages and entries per page

You can click Previous page and Next page button to jump to the tunnel that you want to see. You also can enter the page number into “Jump to page” directly and choose the item number that you want to see per page (3, 5, 10, 20, 50, All).

Tunnel No.: It shows the used Tunnel No. 1~50, and it includes the tunnels defined in GroupVPN.

Name: It shows the Tunnel Name that you enter in Gateway to Gateway page, Client to Gateway page or Group ID Name.

Status: It shows Connected, Hostname Resolution Failed, Resolving Hostname or Waiting for Connection. If users select Manual in IPSec Setup page, the Status will show Manual and no Tunnel Test function for Manual Keying Mode.

Phase2 Encrypt/Auth/Group: It shows the Encryption (DES/3DES), Authentication (MD5/SHA1) and Group (1/2/5) that you chose in IPSec Setup field.
If you chose Manual mode, there will be no Phase 2 DH Group, and it will show the Encryption and Authentication method that you set up in Manual mode.

Local Group: It shows the IP and subnet of Local Group.

Remote Group: It shows the IP and subnet of Remote Group.

Remote Gateway: It shows the IP of Remote Gateway.

Tunnel Test: Click the Connect button to verify the tunnel status. The test result will be updated in Status.

Configure: Edit and Delete 
If you click Edit button, it will link to the original setup page. You can change the settings. If you click  , all settings of this tunnel will be deleted, and this tunnel will be available.

Tunnel(s) Enable and Tunnel(s) Defined: It shows the amount of Tunnel(s) Enable and Tunnel(s) Defined. The amount of Tunnel Enable may be fewer than the amount of Tunnel Defined once the Defined Tunnels are disabled.

Configuring an IPSec Proposal

An IKE proposal contains values for Phase 1 IPSec negotiations. During Phase 1 the two peers establish a secure tunnel within which they then negotiate the Phase 2 parameters. The RV082 VPN Router uses IKE proposals both as initiator and responder in IPSec negotiations.

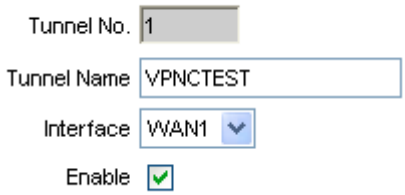
By setting this page, users can add the new tunnel between two VPN devices.

Tunnel No.: The tunnel number will be generated automatically from 1~50.

Tunnel Name: Enter the Tunnel Name, such as LA Office, Branch Site, Corporate Site, etc. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

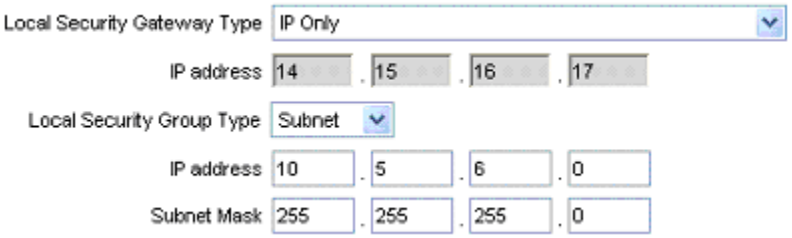
Interface: You can select the Interface from the pull-down menu. When dual WAN is enable, there will be two options. (WAN1/WAN2).

Enable: Check the box to enable VPN.



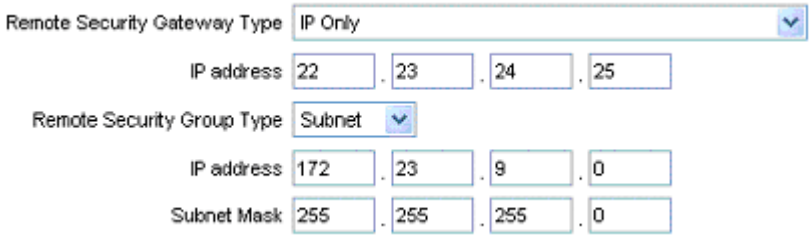
Local Group Setup

Select the local LAN user(s) behind the router that can use this VPN tunnel. Local Security Group Type may be a single **IP** address, a **Subnet** or an **IP range**. The Local Secure Group must match the other router's Remote Secure Group. Please select Subnet as Local Security Group Type here. This will allow all computers on the local subnet to access the tunnel. Enter the IP Address and the Subnet Mask. The default IP is 192.168.1.0, and default Subnet Mask is 255.255.255.192.



Remote Group Setup:

Remote Security Group Type: Select the Remote Security Group that behind the above Remote Gateway Type you chose that can use this VPN tunnel. **Remote Security Group Type** may be a single **IP** address, a **Subnet** or an **IP range**. Please select Subnet as Remote Security Group Type here. This will allow all computers on the remote subnet to access the tunnel. Enter the remote IP Address and the Subnet Mask. The default Subnet Mask is 255.255.255.0.

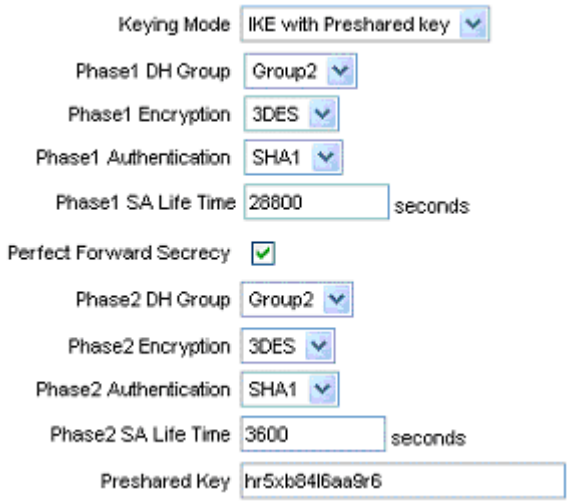


In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a “key” to the encryption code. There

are two Keying Modes of key management, **Manual** and **IKE with Preshared Key** (automatic).
Encryption: There are two methods of encryption, **DES** and **3DES**. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. 3DES is recommended because it is more secure, and both sides must use the same Encryption method.

Authentication: There are two methods of authentication, **MD5** and **SHA**. The Authentication method determines a method to authenticate the ESP packets. MD5 is a one-way hashing algorithm that produces a 128-bit digest. SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure, and both sides must use the same Authentication method.

IKE with Pre-shared Key (automatic)



IKE is an Internet Key Exchange protocol that used to negotiate key material for SA (Security Association). IKE uses the Pre-shared Key field to authenticate the remote IKE peer.

Phase 1 DH Group: Phase 1 is used to create a security association (SA). DH (Diffie-Hellman) is a key exchange protocol that used during phase 1 of the authentication process to establish pre-shared keys. There are three groups of different prime key lengths. **Group 1** is 768 bits, **Group 2** is 1,024 bits and **Group 5** is 1,536 bits. If network speed is preferred, select Group 1. If network security is preferred, select Group 5.

Phase 1 Encryption: There are two methods of encryption, **DES** and **3DES**. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. Both sides must use the same Encryption method. 3DES is recommended because it is more secure.

Authentication: There are two methods of authentication, **MD5** and **SHA**. The Authentication method determines a method to authenticate the ESP packets. Both sides must use the same Authentication method. MD5 is a one-way hashing algorithm that produces a 128-bit digest.
SHA is a one-way hashing algorithm that produces a 160-bit digest. SHA is recommended because it is more secure.

Perfect Forward Secrecy: If PFS is enabled, IKE Phase 2 negotiation will generate a new key material for IP traffic encryption and authentication. If PFS is enabled, a hacker using brute force to break encryption keys is not able to obtain other or future IPSec keys.

Phase 2 DH Group: There are three groups of different prime key lengths. **Group1** is 768 bits, **Group2** is 1,024 bits and **Group 5** is 1,536 bits. If network speed is preferred, select Group 1. If

network security is preferred, select Group 5. You can choose the different Group with the Phase 1 DH Group you chose. If Perfect Forward Secrecy is disabled, there is no need to setup the Phase 2 DH Group since no new key generated, and the key of Phase 2 will be same with the key in Phase 1.

Phase 2 Encryption: Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions. There are two methods of encryption, **DES** and **3DES**. The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. DES is 56-bit encryption and 3DES is 168-bit encryption. Both sides must use the same Encryption method.

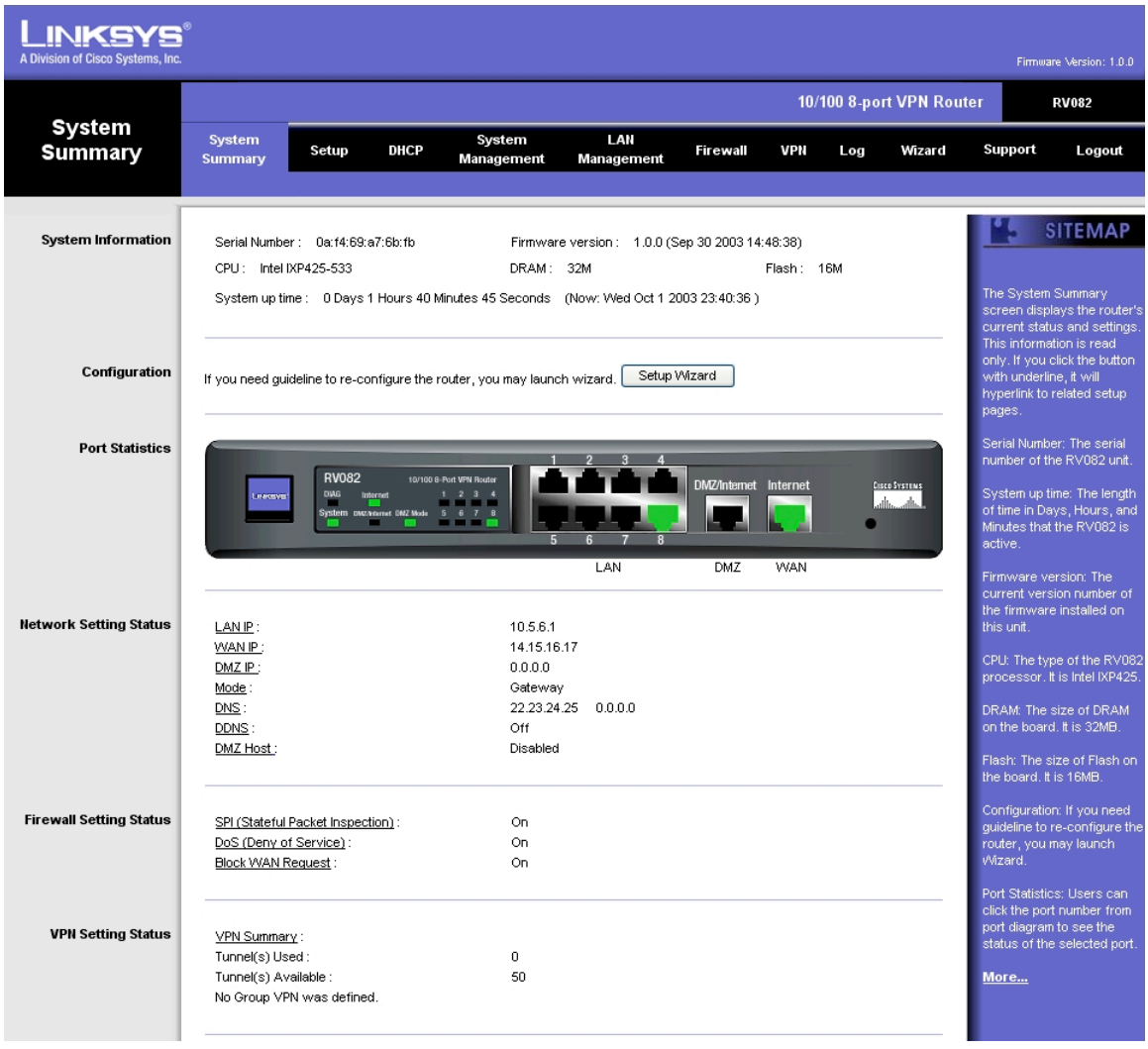
Authentication: There are two methods of authentication, **MD5** and **SHA**. The Authentication method determines a method to authenticate the ESP packets. Both sides must use the same Authentication method. MD5 is a one-way hashing algorithm that produces a 128-bit digest.
SHA is a one-way hashing algorithm that produces a 160-bit digest.

SA Life Time: This field allows you to configure the length of time a VPN tunnel is active. The default value is 3,600 seconds.

Preshared Key: The character and hexadecimal values are acceptable in this field, e.g. "My_@123" or "4d795f40313233." Both sides must use the same Pre-shared Key. It's recommended to change Preshared keys regularly to maximize VPN security.
Clink the **Save Settings** button to save the settings or click the **Cancel Change** button to undo the changes.

EXAMPLE: VPN IPSec Tunnel Configuration

You can also reference the following example to setup IPSec tunnel with VPNC gateway. This setting is based on the portfolio shown on page 1.



Linksys Copy right reserved.