

# IPsec ESP Wildcard Forwarding on RV042, RV042G and RV082 VPN Routers

## Objective

IPsec ESP Wildcard Forwarding establishes a private network between two computers on different networks using a wildcard key. A wildcard pre-shared key allows a group of remote users with the same level of authentication to share an Internet Key Exchange (IKE) pre-shared key without the use of remote peer's IP address.

A wild card mask matches (wildly with a zero) everything in the network portion of an IP address. Internet Protocol Security (IPsec) Encapsulating Security Payload (ESP) is used to route internet traffic across the VPN. It provides data confidentiality, data integrity, and data authentication between participating peers at the IP layer.

This article guides on how to configure an IPsec ESP Wildcard Forwarding on two computers at two sites having two different ISPs connected with RV042, RV042G and RV082 Series VPN Routers.

## Applicable Devices

- RV042
- RV042G
- RV082

## IPsec ESP Wildcard Forwarding

### Site 1 Configuration

Step 1. For Site 1, you need to configure your WAN settings. To know more on how to configure WAN settings refer to *Edit WAN Connection on RV016, RV042, RV042G and RV082 VPN Routers*.

Step 2. Log in to the web configuration utility and choose **VPN > Summary**. The *Summary* page opens:

**Summary**



0 Tunnel(s) Used      100 Tunnel(s) Available      [Details](#)

---

**Tunnel Status**

1 Tunnel(s) Enabled      1 Tunnel(s) Defined

Items 1-1 of 1 Rows per page : 5

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	tunnel_new	waiting for connection	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.1.0 255.255.255.0	192.168.1.5	<a href="#">Connect</a>	 

[Add](#)      Page 1 of 1

---

**Group VPN Status**

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.
<a href="#">Add</a>							

---

**VPN Client Status**

Items 1-1 of 1 Rows per page : 5

No.	Username	Status	Start Time	End Time	Duration
<a href="#">Add</a>					

Page 1 of 1

**Summary**

0 Tunnel(s) Used      100 Tunnel(s) Available      [Details](#)

---

**Tunnel Status**

1 Tunnel(s) Enabled      1 Tunnel(s) Defined

Items 1-1 of 1 Rows per page : 5

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	tunnel_new	waiting for connection	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.1.0 255.255.255.0	192.168.1.5	<a href="#">Connect</a>	 

[Add](#)      Page 1 of 1

---

**Group VPN Status**

Group Name	Connected Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote Client Status	Tunnel Test	Config.
<a href="#">Add</a>							

---

**VPN Client Status**

Items 1-1 of 1 Rows per page : 5

No.	Username	Status	Start Time	End Time	Duration
<a href="#">Add</a>					

Page 1 of 1

Step 3. Click the **Edit** configuration icon under Config, to edit the VPN configuration for site 1. The *Gateway To Gateway* page opens:

### Gateway To Gateway

**Add a New Tunnel**

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

---

**Local Group Setup**

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

---

**Remote Group Setup**

Remote Security Gateway Type :

IP Address :

Remote Security Group Type :

IP Address :

Subnet Mask :

**Local Group Setup**

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

Step 4. Scroll down to *Local Group Setup* section and enter the wildcard IP address, 0.0.0.0 in the IP Address field.

**Note:** The 0.0.0.0 IP address indicates that any remote peer configured with the shared key may establish a connection with the local peer, regardless of the IP address configured on the remote peer.

Step 5. At the Subnet Mask field, enter the wildcard mask, 0.0.0.0.

Step 6. Click **Save** to save the settings.



**Note:** To know more on how to configure gateway-to-gateway VPN refer to *Configuration of*

## Site 2 Configuration

Step 1. For Site 2, you need to configure your WAN settings. To know more on how to configure WAN settings refer to *Edit WAN Connection on RV016, RV042, RV042G and RV082 VPN Routers*.

Step 2. Log in to the web configuration utility and choose **VPN > Summary**. The *Summary* page opens:

The screenshot shows the 'Summary' page of the VPN configuration utility. At the top, it displays '0 Tunnel(s) Used' and '100 Tunnel(s) Available' with a 'Details' button. Below this is the 'Tunnel Status' section, showing '1 Tunnel(s) Enabled' and '1 Tunnel(s) Defined'. A table lists the tunnel configuration:

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	tunnel_2	waiting for connection	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.1.0 255.255.255.0	192.168.1.0	Connect	 

Below the table is an 'Add' button and pagination controls showing 'Page 1 of 1'. The 'Group VPN Status' section is empty. The 'VPN Client Status' section is also empty.

This screenshot is identical to the one above, but with a red circle highlighting the edit icon (a pencil) in the 'Config.' column of the tunnel configuration table.

Step 3. Click the Edit Configuration **icon** under Config icon to edit the VPN configuration for site 2. The *Gateway To Gateway* page opens:

**Remote Group Setup**

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.0

Remote Security Group Type : Subnet

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Step 4. Scroll down to *Remote Group Setup* and enter the wildcard IP address, 0.0.0.0 in the IP Address field.

**Note:** The 0.0.0.0 IP address indicates that any remote peer configured with the shared key may establish a connection with the local peer, regardless of the IP address configured on the remote peer.

Step 5. At the Subnet Mask field, enter the wildcard mask, 0.0.0.0.

Step 6. Click **Save** to save the settings.

**Note:** To know more on how to configure gateway-to-gateway VPN refer to *Configuration of Gateway to Gateway VPN on RV016, RV042, RV042G and RV082 VPN Routers*.