



Hewlett Packard
Enterprise

HPE IMC

Building IPsec VPNs with IVM and BIMS Configuration Examples

Part number: 5200-1350
Software version: IMC IVM 7.2 (E0402)

The information in this document is subject to change without notice.
© Copyright 2016 Hewlett Packard Enterprise Development LP

Contents

Introduction.....	1
Prerequisites	1
Configuration restrictions and guidelines	2
Example: Using IVM and BIMS to build an IPsec VPN	2
Network requirements	2
Configuring BIMS service parameters	2
Importing Router A and Router B to IVM	3
Configuring global IPsec settings for Router A and Router B	4
Configuring an IPsec VPN domain.....	5
Adding an IPsec VPN domain	5
Adding an IPsec tunnel in the VPN domain	7
Deploying the IPsec tunnel.....	10
Enabling monitoring for the IPsec tunnel	11
Related documentation.....	11

Introduction

This document provides an example for using IVM and BIMS to build an IPsec VPN.

IVM provides solutions to managing IPsec VPNs and DVPNs for enterprise headquarters and branches. BIMS uses TR-069 to manage CPEs.

IVM can import IPsec devices from BIMS and configure, deploy, and monitor the IPsec devices through BIMS.

Prerequisites

Before you use IVM and BIMS to build an IPsec VPN, perform the following configurations:

- Deploy the IMC Platform, IVM, and BIMS.
- Add the hub and spokes to the IMC Platform, and configure SNMP and Telnet on the hub so IMC can manage the hub.
- Use the following commands to configure CWMP on the spokes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter CWMP view.	cwmp	N/A
3. Enable CWMP.	cwmp enable	Optional. By default, CWMP is enabled.
4. Specify the URL of the ACS.	cwmp acs url <i>url</i>	By default, no ACS URL is specified.
5. Configure the username for authentication with the ACS.	cwmp acs username <i>username</i>	By default, no username is configured.
6. Configure the password for authentication with the ACS.	cwmp acs password <i>password</i>	By default, no password is configured for authentication with the ACS. You can specify a username without a password for authentication, but must make sure the ACS has the same authentication setting as the CPE.

- (Optional.) Configure the CPEs (BIMS devices).
To enable a CPE to authenticate the ACS, configure a username and password on the CPE. Upon receiving a session request from an ACS, the CPE compares the CPE username and password in the session request with the local settings. If they are the same, the ACS passes the authentication, and the connection establishment proceeds. Otherwise, the authentication fails, and the connection establishment is terminated.
- Enable the encryption engine and IPsec module backup function on the IPsec devices.
The encryption engine performs IPsec processing. If the encryption engine is disabled or has failed but the IPsec module backup function is enabled, the IPsec module performs IPsec processing. If the IPsec module backup function is disabled, IPsec packets are discarded.
To enable the encryption engine and IPsec module backup function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enable the encryption engine.	cryptoengine enable	Optional. The default setting depends on the device model.
3. Enable the IPsec module backup function.	ipsec cpu-backup enable	Required. By default, the IPsec module backup function is enabled.

Configuration restrictions and guidelines

Only one administrator can perform deployment operations in a VPN domain at a time.

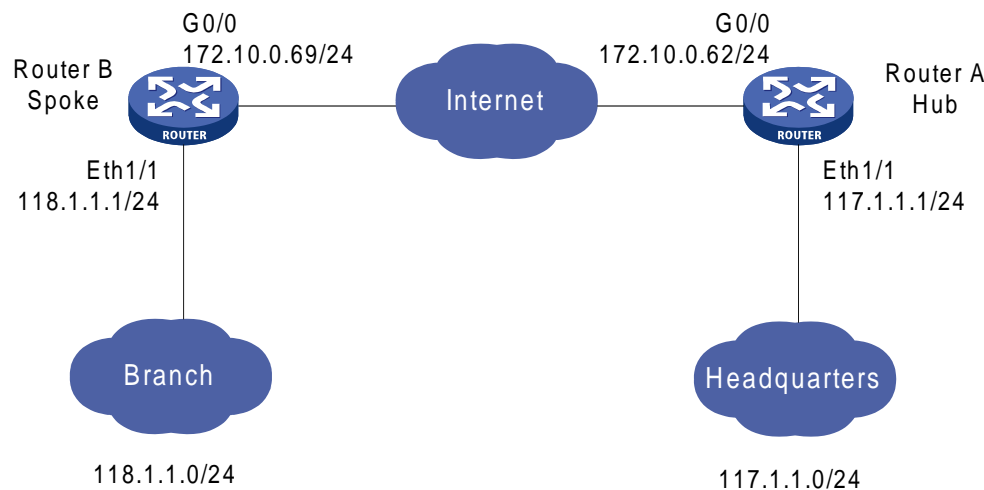
Example: Using IVM and BIMS to build an IPsec VPN

Network requirements

As shown in [Figure 1](#), Router A and Router B are added to the IMC Platform. Router B is configured with CWMP and managed by BIMS.

Establish an IPsec tunnel between Router A (the hub) and Router B (the spoke) to protect data flows between subnet 117.1.1.0/24 and subnet 118.1.1.0/24.

Figure 1 Network diagram



Configuring BIMS service parameters

1. Click the **Service** tab.
2. From the navigation tree, select **IPsec VPN Manager > Options**.
The **BIMS Service Settings** tab page appears, as shown in [Figure 2](#).
3. Select the **Enable BIMS** option.
4. Configure the BIMS server address, username and password.

The BIMS server address must be the same as the ACS URL configured on Router B.

5. Click **Test** to test connectivity to the BIMS server.
6. Click **OK**.

Figure 2 Configuring BIMS service parameters

Service > IPsec VPN Manager > Options ★ Add to My Favorites ? Help

BIMS Service Settings | BIMS Device Settings | Monitor Settings

Enable BIMS

BIMS Server Address ?

User Name

Password

Test

OK

7. Use the default settings on the **BIMS Device Settings** tab and **Monitor Settings** tab.

Importing Router A and Router B to IVM

1. Click the **Service** tab.
2. From the navigation tree, select **IPsec VPN Manager > IPsec Resources > IPsec Devices**. The **IPsec Devices** page appears.
3. Click **Import**. The **Import IPsec Devices** page appears.
4. Import Router A to IVM:
 - a. Click **Select Devices**. The **Select Device** window appears.
 - b. Select Router A (identified by IP address 172.10.0.62) and click **OK**. Router A appears in the **Device List**, as shown in [Figure 3](#).

Figure 3 Importing Router A to IVM

Service > IPsec VPN Manager > IPsec Devices > Import IPsec Devices ? Help

Device List

Select Devices | Select BIMS Device | Delete

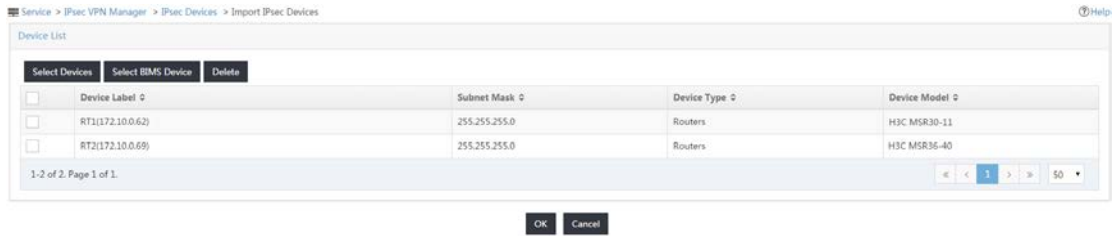
Device Label	Subnet Mask	Device Type	Device Model
RT1(172.10.0.62)	255.255.255.0	Routers	H3C MSR30-11

1-1 of 1, Page 1 of 1 < > 50

OK **Cancel**

5. Import Router B to IVM:
 - a. Click **Select BIMS Device**. The **Select BIMS Device** window appears.
 - b. Select Router B (identified by IP address 172.10.0.69) and click **OK**. Router B appears in the **Device List**, as shown in [Figure 4](#).

Figure 4 Importing Router B to IVM

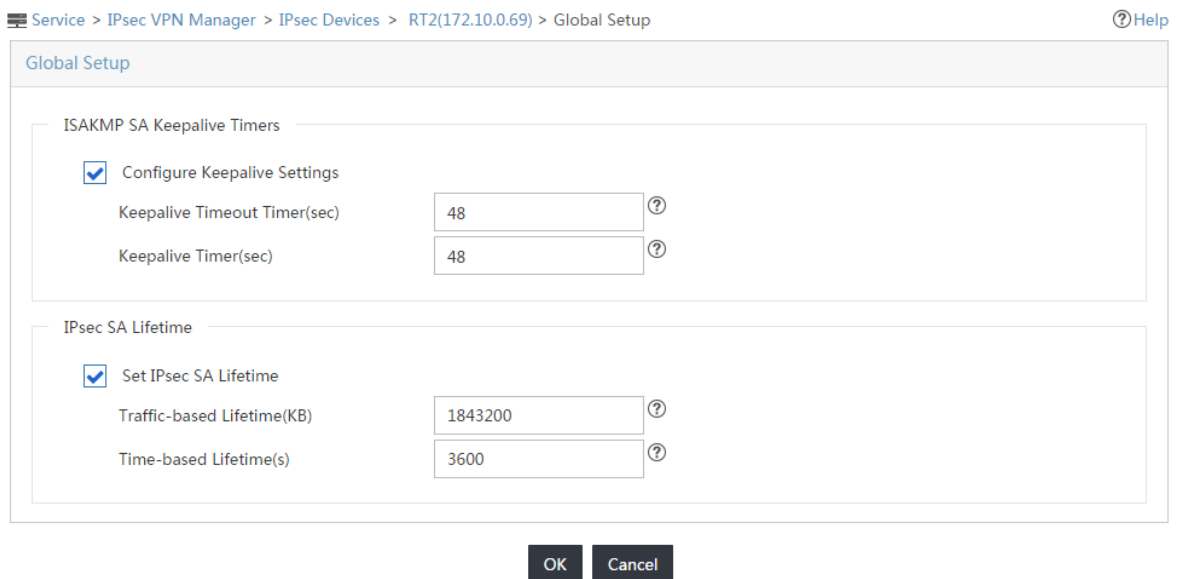


6. Click **OK** to start importing Router A and Router B to IVM.
IVM displays the import result after the operation is complete.

Configuring global IPsec settings for Router A and Router B

1. Click the **Service** tab.
2. Select **IPsec VPN Manager > IPsec Resources > IPsec Devices** from the left navigation tree.
The **IPsec Device List** displays all IPsec devices.
3. Click the **Operation** icon "⋮" for Router B, which is identified by a device label of **MSR3040(172.10.0.69)**.
4. Select **Global Setup** from the shortcut menu.
The **Global Setup** page appears.
5. Configure the global settings, as shown in [Figure 5](#), and click **OK**.

Figure 5 IPsec global settings



6. Repeat steps 3 to 5 to configure IPsec global settings for Router A.
7. Select Router A and Router B, and click **Synchronize** to deploy the configurations to the devices.

Configuring an IPsec VPN domain

Adding an IPsec VPN domain

1. Click the **Service** tab.
2. From the navigation tree, select **IPsec VPN Manager > IPsec Resources > VPN Domains**. The **VPN Domains** page appears.
3. Click **Add** to display the add VPN domain wizard.
4. Add a VPN domain named **IVM-BIMS**.

Configure the basic settings and default IPsec and IKE settings for the domain, as shown in [Figure 6](#).

Figure 6 Adding an IPsec VPN domain

Service > IPsec VPN Manager > VPN Domains > Add VPN Domain > 1. Configure Basic Settings > 2. Configure Security Proposals Help

Configure Basic Settings

Basic information

Domain Name *

Description

Type IPsec VPN GRE over IPsec DVPN

Configure IPsec and IKE

Use default IPsec and IKE configurations

IKE Negotiation Mode Main Aggressive

NAT Traversal YES NO

IKE Authentication Pre-Shared Key CA Authentication

Authentication Key ?

ID Type IP Name

Encapsulation Mode Tunnel Transport

Use Policy Template YES NO

PFS ▼

Set IPsec SA Lifetime YES NO

5. Click **Next** to display the **Configure Security Proposals** page, as shown in [Figure 7](#).

Figure 7 Configuring security proposals

Service > IPsec VPN Manager > VPN Domains > Add VPN Domain > 1. Configure Basic Settings > 2. Configure Security Proposals ? Help

Configure Security Proposals

IPsec Proposal

Add **Delete**

<input type="checkbox"/>	Proposal Name	Encapsulation	Security Protocol	AH AuthN	ESP AuthN	ESP Encrypt	Modify
No match found.							

IKE Proposal

Add **Delete**

<input type="checkbox"/>	Proposal Num.	IKE Authentication	Encryption Algorithm	Authentication Algorithm	DH Group ID	ISAKMP SA Lifetime	Modify
No match found.							

Previous **Accomplish** **Cancel**

6. Add an IPsec proposal:
 - a. Click **Add** in the **IPsec Proposal** area.

The **Add IPsec Proposal** window appears, as shown in [Figure 8](#).
 - b. Configure the IPsec proposal parameters and click **OK**.

Figure 8 Adding an IPsec proposal

Service > IPsec VPN Manager > VPN Domains > Add VPN Domain > 1. Configure Basic Settings > 2. Configure Security Proposals ? Help

Add IPsec Proposal

Proposal Name * ?

Encapsulation Tunnel Transport

Security Protocol

ESP AuthN

ESP Encrypt

OK **Cancel**

7. Add an IKE proposal:
 - a. Click **Add** in the **IKE Proposal** area.

The **Add IKE Proposal** window appears, as shown in [Figure 9](#).
 - b. Configure the IKE proposal parameters and click **OK**.

Figure 9 Adding an IKE proposal

Service > IPsec VPN Manager > VPN Domains > Add VPN Domain > 1. Configure Basic Settings > 2. Configure Security Proposals Help

Add IKE Proposal

Proposal Num. ?

IKE Authentication Pre-Shared Key CA Authentication

Encryption Algorithm

Authentication Algorithm

DH Group ID

ISAKMP SA Lifetime ?

8. Click **Accomplish**.

Adding an IPsec tunnel in the VPN domain

1. On the **VPN Domain List**, click the name of the VPN domain **IVM-BIMS**.
The **Tunnel List** page of the VPN domain appears, as shown in [Figure 10](#).

Figure 10 Tunnel list

Service > IPsec VPN Manager > VPN Domains > IVM-BIMS Help

VPN Domain Information

Name: IVM-BIMS

Query Tunnels

Hub Name: Hub IP: Advanced Query

Spoke Name: Spoke IP:

Tunnel List

<input type="checkbox"/>	Hub Device	Hub Interface(Gateway IP)	Spoke Device	Spoke Interface(Gateway IP)	Status	Monitoring Data	Configuration	Operation
No match found.								

0-0 of 0. Page 1 of 1. < > 50

2. Click **Add** in the **Tunnel List** area.
3. Click **Select Hub**. The **Select Hub** window appears. Select Router A and click **OK**.
The **Hub Device Information** area appears on top of the tunnel list, as shown in [Figure 11](#).

Figure 11 Selecting the hub

Service > IPsec VPN Manager > VPN Domains > IVM-BIMS > Add Tunnel Help

Hub Device Information

Hub Device: RT1(172.10.0.62)

Tunnel List

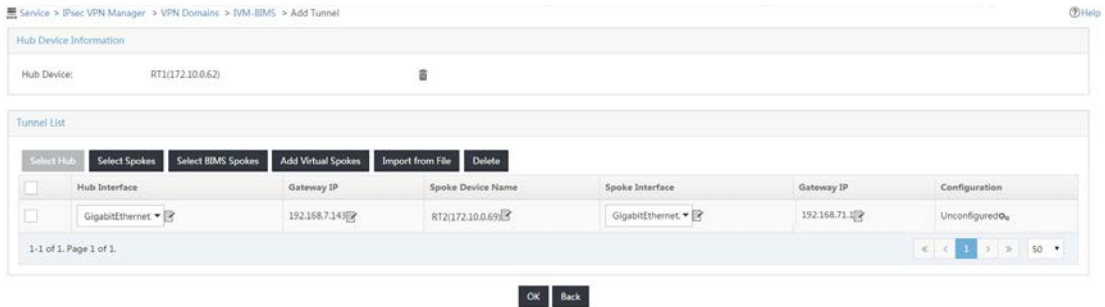
<input type="checkbox"/>	Hub Interface	Gateway IP	Spoke Device Name	Spoke Interface	Gateway IP	Configuration
No match found.						

0-0 of 0. Page 1 of 1. < > 50

4. Click **Select BIMS Spokes**. The **Select BIMS Spokes** window appears. Select Router B and click **OK**.

IVM automatically generates an unconfigured hub-spoke tunnel between Router A and Router B, as shown in [Figure 12](#).

Figure 12 Selecting the spoke



5. Modify the names and IP addresses of the hub interface and spoke interface, as shown in [Figure 13](#).


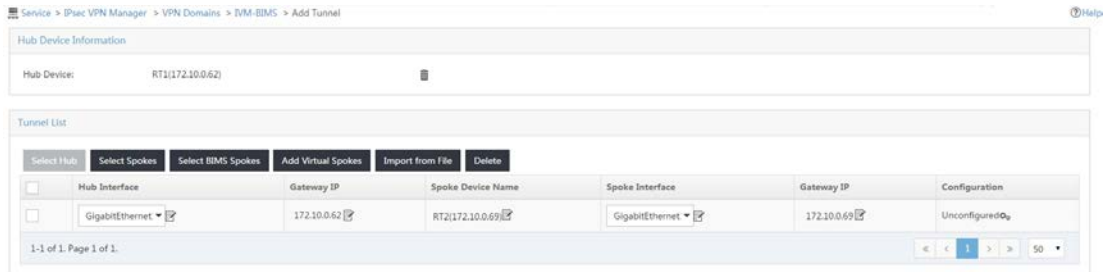
For example, to modify the hub interface name, click the **Modify** icon , select **GigabitEthernet0/0** in the text box and click **OK**.

Figure 13 Configuring interfaces and IP addresses for the IPsec tunnel




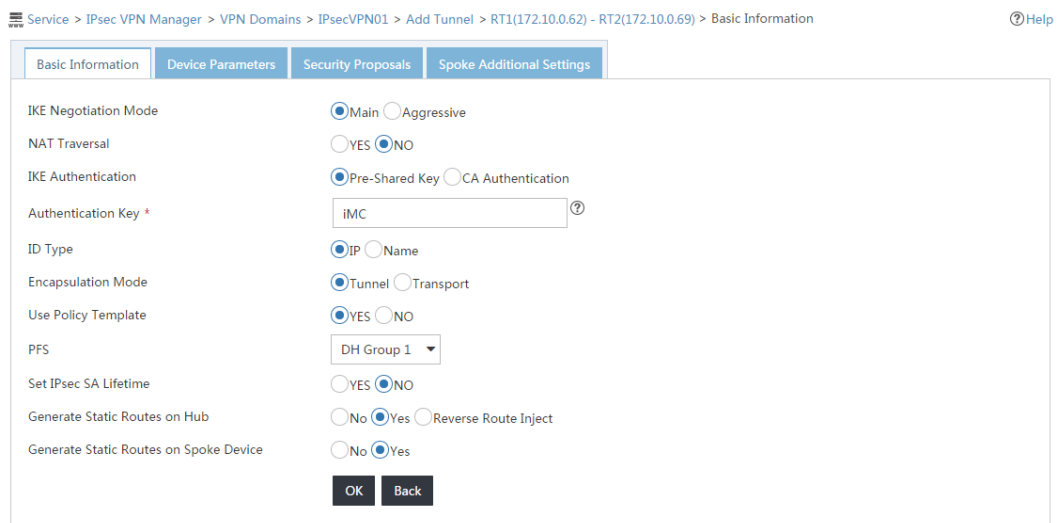
6. Configure the IPsec tunnel:
 - a. In the **Operation** column, click the **Device Parameters** icon  to display the tunnel configuration page, as shown in [Figure 14](#).
 - b. Configure the basic information, as shown in [Figure 14](#) and click **OK**.

Figure 14 Configuring basic information



- a. Click the **Device Parameters** tab, and click **Add** to display the **Add Protected Traffic Flows** window.
- b. Add a protected traffic flow, as shown in [Figure 15](#), and click **OK**.

Figure 15 Adding protected traffic flows

Add Protected Traffic Flows

Protocol: IP

Hub Subnet Address *: 117.1.1.0

Hub Subnet Mask *: 255.255.255.0

Spoke Subnet Address *: 118.1.1.0

Spoke Subnet Mask *: 255.255.255.0

OK Cancel

- c. Use the default settings on the **Security Proposals** tab and **Spoke Additional Settings** tab, as shown in [Figure 16](#) and [Figure 17](#).

Figure 16 Security proposals tab

Service > IPsec VPN Manager > VPN Domains > IPsecVPN01 > Add Tunnel > RT1(172.10.0.62) - RT2(172.10.0.69) > Security Proposals

Basic Information Device Parameters Security Proposals Spoke Additional Settings

IPsec Proposals

Add Delete

Hub Proposal	Spoke Proposal	Encapsulation	Security Protocol	AH AuthN	ESP AuthN	ESP Encrypt	Hub Encrypt-card Slot	Spoke Encrypt-card Slot
IPsec01	IPsec01	Tunnel	ESP	None	MDS	DES		-

IKE Proposals

Add Delete

Hub Proposal No.	Spoke Proposal No.	IKE Authentication	Encryption Algorithm	Authentication Algorithm	DH Group ID	ISAKMP SA Lifetime
1	1	Pre-Shared Key	DES	SHA1	DH Group 1	86400

Back

Figure 17 Spoke additional settings tab

Service > IPsec VPN Manager > VPN Domains > IPsecVPN01 > Add Tunnel > RT1(172.10.0.62) - RT2(172.10.0.69) > Spoke Additional Settings

Basic Information Device Parameters Security Proposals Spoke Additional Settings

IP Address of the Spoke Interface

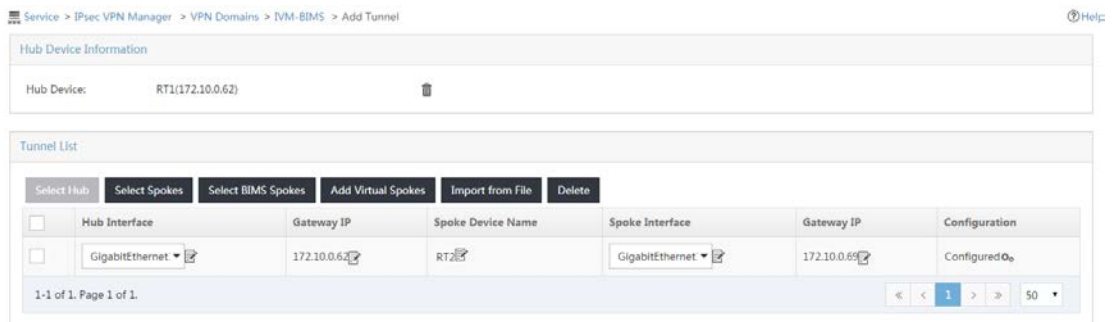
DHCP Relay

User-Defined Settings

OK Back

- Click **Back** to return to the tunnel list page.
The **Configuration** column of the tunnel changes to **Configured**, as shown in [Figure 18](#).

Figure 18 Tunnel list page

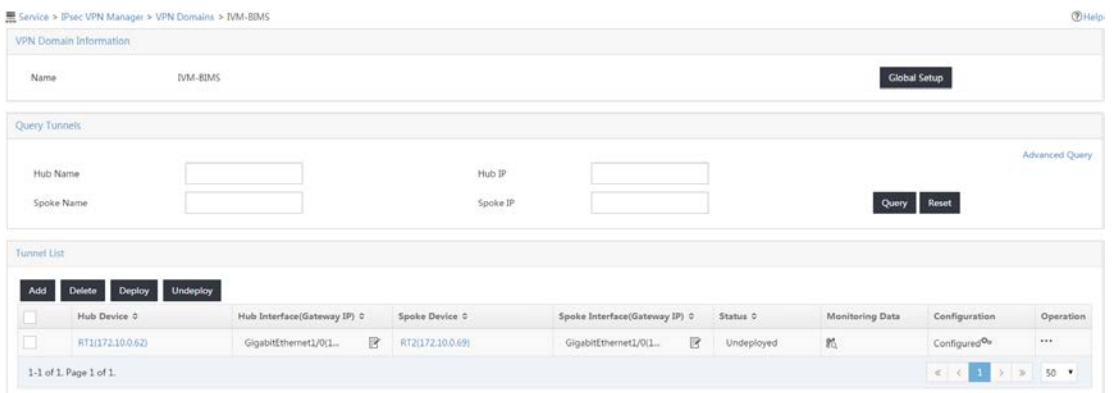


- Click **OK**.

Deploying the IPsec tunnel

- Select the hub-spoke IPsec tunnel between Router A and Router B and click **Deploy**, as shown in [Figure 19](#).

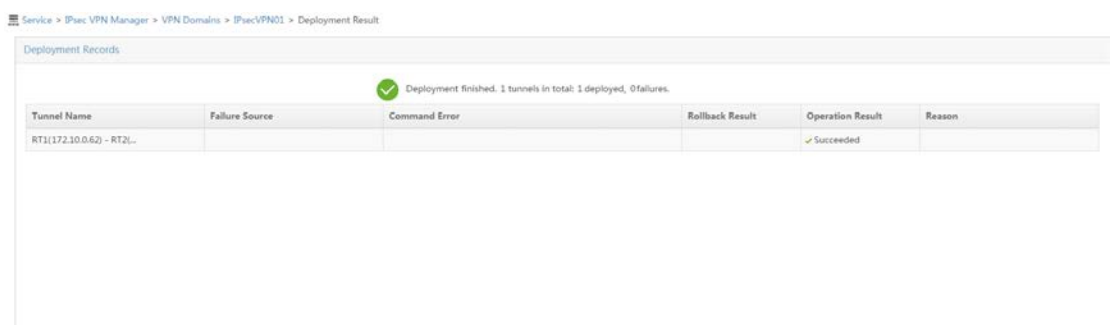
Figure 19 Deploying the IPsec tunnel



The page displays the operation result, as shown in [Figure 20](#). If a failure occurs, the failure reason is displayed.

After a tunnel is successfully deployed to the devices, the tunnel status in IVM changes to **Ready**.

Figure 20 Deployment result



Enabling monitoring for the IPsec tunnel

1. Click the **Service** tab.
2. From the navigation tree, select **IPsec VPN Manager > IPsec Resources > IPsec Tunnels**.
The **Tunnel List** displays all IPsec tunnels, as shown in [Figure 21](#).


Figure 21 IPsec tunnels

The screenshot shows the 'IPsec Tunnels' management page. At the top, there are tabs for 'Active Tunnels' and 'History Tunnels'. Below the tabs is a 'Query Tunnels' section with input fields for 'Device Name', 'Tunnel Name', 'Local IP', 'Device IP', 'Monitored' (a dropdown menu set to 'All'), and 'Remote IP'. There are 'Query' and 'Reset' buttons. Below the query section is the 'Tunnel List' table. The table has columns for 'Tunnel Status', 'Monitored', 'Device Name', 'Tunnel Name', 'Type', 'Local IP/Subnet', 'Remote IP/Subnet', 'Rx Rate (bps)', 'Tx Rate (bps)', and 'Monitoring Data'. There are also buttons for 'Monitor ON', 'Monitor OFF', and 'Delete' above the table. The table contains two rows of IPsec tunnels, both with 'Monitored' status set to 'No'. The first row has Local IP/Subnet 172.10.0.69/118.1.1.1 and Remote IP/Subnet 172.10.0.62/117.1.1.1. The second row has Local IP/Subnet 172.10.0.62/117.1.1.1 and Remote IP/Subnet 172.10.0.69/118.1.1.1. The 'Monitoring Data' column contains an icon for each row. At the bottom, there is a pagination control showing '1-2 of 2, Page 1 of 1' and a search box with '50'.

3. Select the IPsec tunnel and click **Monitor ON**.
The **Monitored** column of the tunnel changes to **Yes**, as shown in [Figure 22](#).

Figure 22 Enabling monitoring for the IPsec tunnel

This screenshot is identical to Figure 21, but the 'Monitored' status for the first tunnel (Local IP/Subnet 172.10.0.69/118.1.1.1) has changed to 'Yes'. The 'Rx Rate (bps)' and 'Tx Rate (bps)' columns now show values: 231.03K and 225.23K respectively. The 'Monitoring Data' icon for this row is now active.

After you enable monitoring for an IPsec tunnel, you can view the tunnel receive and transmit rates in a specified time period by clicking the **Monitoring Data** icon .

Related documentation

HPE IMC IPsec VPN Manager Administrator Guide
HPE Intelligent Management Center IVM Online Help