Configuring Services: IPSec VPN Menu

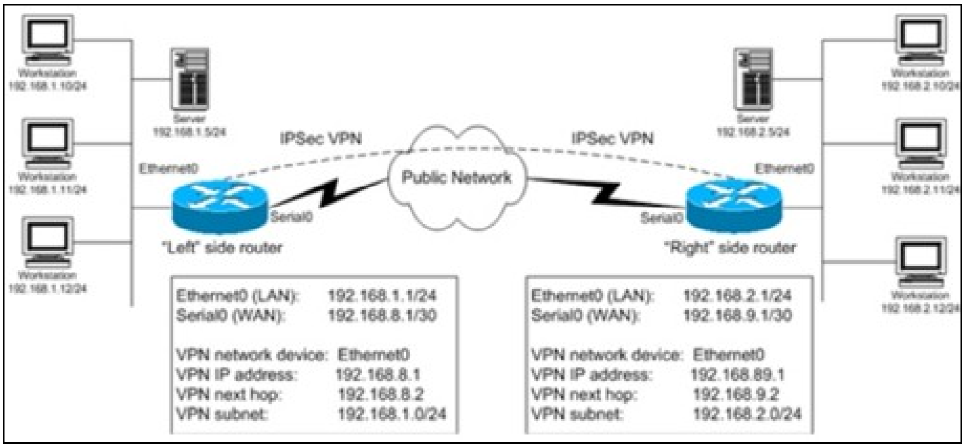
Version: 3507

Table of Contents

Router Installation and Configuration Manual/Configuring Services: IPSec VPN Menu

This chapter describes how to configure the IPSec Virtual Private Network (VPN) service on the ImageStream Router. IPSec is a Internet Protocol Security. It uses strong cryptography to provide both authentication and encryption services. Authentication ensures that packets are from the proper sender and have not been altered in transit. Encryption prevents unauthorized reading of packet contents.

These services allow you to build secure tunnels through untrusted networks, such as a public Frame Relay network or Internet backbone network. All traffic passing through the untrusted network is encrypted by the IPSec gateway and decrypted by the gateway at the other end. The result is Virtual Private Network or VPN. This is a network which is effectively private even though it includes machines at several different sites connected by an insecure network. This chapter outlines a simple network-to-network connection.


Workstation
192.168.1.10/24
Workstation
192.168.1.11/24
Workstation
192.168.1.12/24
Server
192.168.1.5/24
Ethernet0
Serial0
"Left" side router
IPSec VPN
Public Network
IPSec VPN
Server
192.168.2.5/24
Ethernet0
Serial0
"Right" side router
Workstation
192.168.2.10/24
Workstation
192.168.2.11/24
Workstation
192.168.2.12/24
Ethernet0 (LAN): 192.168.1.1/24
Serial0 (WAN): 192.168.8.1/30
VPN network device: Ethernet0
VPN IP address: 192.168.8.1
VPN next hop: 192.168.8.2
VPN subnet: 192.168.1.0/24
Ethernet0 (LAN): 192.168.2.1/24
Serial0 (WAN): 192.168.9.1/30
VPN network device: Ethernet0
VPN IP address: 192.168.89.1
VPN next hop: 192.168.9.2
VPN subnet: 192.168.2.0/24

More advanced configurations are possible. This chapter includes the following topics:

- ◊ Configuring the IPSec VPN service
- ◊ Enabling the IPSec VPN service at boot-time
- ◊ Disabling the IPSec VPN service at boot-time
- ◊ Starting the IPSec VPN service
- ◊ Stopping the IPSec VPN service

After logging in, the main menu is displayed (your menu may look slightly different):

```
ISis-Router main menu
1. Configuration menu
```

```
2. Show interface status
3. Advanced
4. Router software management
5. Backup/Restore
6. halt/reboot
0. Log off
```

Select menu option 1, Configuration menu, and press **Enter** to configure the router. The Configuration menu should appear (your menu may look slightly different):

```
Configuration menu
1. AAA (Password) Configuration
2. Global configuration
3. Network interface configuration
4. Firewall and QOS configuration
5. Service configuration
6. Dynamic routing configuration
7. Save configuration to flash
0. ISis-Router main menu
```

Select menu optioin 5, Service configuration, and press **Enter** to configure the router's service configuration settings. The Service configuration menu will be displayed (again, your menu may look slightly different):

```
Service configuration
1. System scheduler (cron), (running)
2. Dialout PPP, (stopped)
3. IPSec VPN (Free S/Wan), (stopped)
4. NetFlow exporter (nprobe), (stopped)
5. network interfaces (sand), (running)
6. sconsole (mgetty), (running)
7. snmp (net-snmp), (stopped)
8. ssh (OpenSSH), (running)
0. Configuration menu
```

Select menu option 4, IPSec VPN, and press **Enter** to configure the router's IPSec VPN settings. The IPSec VPN menu will be displayed (again, your menu may look slightly different):

```
IPSec VPN (Free S/Wan), (stopped)
1. Configure IPSec (Free S/Wan)
2. Generate a new Signature Key
3. Configure a basic IPSec VPN
4. Enable IPSec on boot
5. Disable IPSec on boot
6. Start IPSec
7. Stop IPSec
0. Service configuration
```

To configure the network-to-network VPN connection, you will need two IPSec-capable gateways with static IP addresses. The IP addresses must be the addresses connecting the gateways to the unsecure network. For example, on a router with a LAN connected to Ethernet0 and a WAN connection through Serial0, the static IP address would be the IP address of the Serial0 device. You will also need a network behind each gateway with non-overlapping IP ranges. Generally, this will be a LAN or a device that connects the gateway to a private, secure network.

Refer to the VPN diagram above or Glossary if you do not understand the terms used in the table below. Before attempting to complete your VPN configuration, you should have the following information ready:

IPSEC VPN Pre-Configuration Information

IPSec VPN Pre-Configuration Information

Ensure that you have the following information ready before you start configuring the VPN.

Parameter	Where to find	Description
Left Side VPN device	Network Diagram	The Router on the left side of the VPN tunnel diagram. This router will always be the "left: side endpoint for the purposes of configuring a VPN connection
Right Side VPN device	Network Diagram	The on the right side of the VPN tunnel diagram. This router will always be the "right" side endpoint for the purposes of configuring a VPN connection
Left and Right Side Network devices	Network Diagram	The LAN or WAN interfaces used as the endpoints of the VPN tunnel. These devices are typically the WAN or LAN devices closest to the external network and not internal LAN or WAN devices
Left and Right Side IP addresses	Line Provider or Network Administrator	The left and right side IP addresses will be IP addresses of the left and right side network devices used for the VPN tunnel endpoints
Left and Right Side Next Hop address	Line Provider or Network Administrator	The left and right side next hop address will be the gateway addresses for the VPN tunnel endpoints
Left and Right Side Subnets	Network Diagram or Network Administrator	The left and right side subnets will be the networks to be connected across the VPN tunnel. These subnets must be non-overlapping

Using the Built-in Automated Script to Configure a VPN Tunnel

To configure a simple IPSec VPN, select menu option 3, Configure a basic IPSec VPN, and press**Enter**. This will start an interactive script that displays the following:

```
Now generating a key for this host (May take some time)...done.
Please see the ImageStream Technical Support Web site
or the ImageStream Router Installation Guide
for details on the information requested by this script.
```

The router will have generated a signature key used to authenticate the VPN connection. The router will then display the following:

```
Will this router be the [L]eft or [R]ight side tunnel endpoint (L/r) ?
```

Enter the correct side for this router. The left and right side designations are not relative to the router. This router will always be either the left side or right side router. Use your network diagram to determine whether this router will act as the left or right side router. For example, if you want to configure this router as the left side router, enter L and **Enter** at this prompt.

The router will then ask you to confirm your choice. In the example below, we have accepted the default configuration and set this router as the left side router:

```
This router will be configured as the left side for this IPSec configuration.   Is this correct (Y/n) :
```

If these values are correct, press 'Y' or leave the entry blank and press **Enter**. If you have made a mistake, press 'N' and **Enter** and the router will reprompt you for the information.

If you pressed 'Y' or '*Enter* the following script will be displayed:

```
Retrieving the public RSA key for this router...done
```

The router will retrieve the public signature key generated earlier. This key will be used in the IPSec configuration file and as part of the authentication process with the other router.

The router will then display:

```
What interface will this router use as the VPN device (default: Ethernet0) ?
```

At this prompt, enter the interface you want to use as the VPN device. Typically, this will be the device closest to the upstream Internet connection on your network. You can press **Enter** to accept the default value, or enter a device name. For example, to use Serial0 as the VPN device, enter **Serial0** at this prompt and press Enter.

The router will then ask you to confirm your choice. In the example below, we have set Serial0 as the VPN device:

```
This router will use Serial0 as the VPN device for this IPSec configuration.   Is this correct (Y/n) :
```

If these values are correct, press 'Y' or leave the entry blank and press **Enter**. If you have made a mistake, press 'N' and **Enter** and the router will reprompt you for the information.

If you pressed 'Y' or Enter, the following script will be displayed:

```
What is the IP address of Serial0 used for IPSec?
```

Enter the primary or secondary IP address used for the VPN tunnel endpoint. For example, to use 192.168.8.1 as the IP address for this side, enter **192.168.8.1** at this prompt and press Enter.

The router will then ask you to confirm your choice. In the example below, we have entered 192.168.8.1:

```
This router will use 192.168.8.1 as the IP address for this IPSec configuration.   Is this correct (Y/n)
```

If these values are correct, press 'Y' or leave the entry blank and press **Enter**. If you have made a mistake, press 'N' and **Enter** and the router will reprompt you for the information.

If you pressed 'Y' or Enter, the following script will be displayed:

```
What is the next hop address for this router?
```

Enter the gateway IP address for this VPN tunnel endpoint. This address should be the one used by the router when traffic leaves the router for the other VPN tunnel endpoint. For example, to use 192.168.8.2 as the IP address for this side, enter **192.168.8.2** at this prompt and press **Enter**.

The router will then ask you to confirm your choice. In the example below, we have entered 192.168.8.2:

```
This router will use 192.168.8.2 as the next hop address for this IPSec configuration.   Is this
```

If these values are correct, press 'Y' or leave the entry blank and press **Enter**. If you have made a mistake, press 'N' and **Enter** and the router will reprompt you for the information.

The following script will then displayed:

```
What is the subnet on this router that is to be accessible across the VPN?

For the next question, please enter the value in the format of "ipnetwork/bitmask"

For example, the Class C 192.168.1.x would be entered as 192.168.1.0/24.

Enter the subnet on this router to be accessible across the VPN :
```

Enter the subnet address for this side of the VPN tunnel. This subnet should be the network you want to make accessible from the other side of the VPN tunnel. For example, to use 192.168.1.0/24 as the subnet for this side, enter **192.168.1.0/24** at this prompt and press **Enter**.

The router will then ask you to confirm your choice. In the example below, we have entered 192.168.1.0/24:

```
This router will use 192.168.1.0/24 as the subnet on this router to be accessible across the VPN.
  Is this correct (Y/n) :
```

If these values are correct, press 'Y' or leave the entry blank and press **Enter**. If you have made a mistake, press 'N' and **Enter** and the router will reprompt you for the information.

Once you have entered the correct values for the first side, the router will then prompt you for the information on the other side of the VPN tunnel. Again, remember that the left and right side designations are not relative to the router. The left side router will always be the left side router and vice versa.

If enter 'Y' or pressed **Enter** the router will display:

```
Next, we will enter the values for the right side router...
```

The router will then prompt you for the identical information for the other side of the VPN tunnel. Please refer to the above section for assistance in answering the questions.

Once you have entered the values for the other endpoint, the router, based on our example, will display:

```
If the right side router is ImageStream, do you want to attempt to get the right side router's public RS
```

If the remote router is ImageStream, you can configure it for the IPSec VPN connection automatically. To use this feature, the router you are configuring must have a network connection to the remote router and the remote router must have a signature key already generated. If you want to attempt to get the remote router's public key, press 'Y' or leave the entry blank and press **Enter**. If the remote router is not ImageStream, or if you do not have access or a connection to it, press 'N' and **Enter** and the script will not attempt to automatically configure the remote router.

Auto Configuring a VPN Tunnel on a Remote ImageStream Router

If you have entered Y or left the entry blank and pressed **Enter** when prompted to get the remote router's public RSA key, the router will prompt you for the IP address of the remote router:

```
Enter the IP address of the right side router :
```

Enter the IP address of the remote router. This address must be accessible to the local router, and the remote router must have SSH enabled and accessible. If you enter an address that is not accessible, or your connection hangs, you will have an opportunity to terminate the connection. In the example below, we have entered 192.168.100.140 as the remote router:

```
Attempting to contact the right side router...
Press Control-\ at any time to interrupt the connection process. Attempting to contact the right side ro
You will be prompted for the password...
Warning: Permanently added '192.168.100.140' (RSA) to the list of known hosts.
root@192.168.100.140's password:
```

Enter the password for the remote router and press Enter. The script will then download the remote router's RSA signature key for use in the VPN configuration process. The router will then display following, based on our example:

```
ipsec.secrets   100% |***       ***|    3814    00:00
Retrieving the public RSA key for the right side router...done Successfully retrieved public RSA key.
Now creating the tunnel configuration for this router...done
```

If there is an error retrieving the key, either because an incorrect IP address was given or the "ipsec.secrets" file was not located, the router will display the following:

```
Unable to locate the IPSec keyfile on the right side router. You must generate a key on the remote route
Would you like to try again? (Y/n) :
```

You can generate an RSA signature key on the remote router, or check the connection to the remote router and try again by pressing 'Y' or by leaving the entry blank and pressing **Enter**. Pressing 'N' and **Enter** will put the router in manual configuration mode. Please see the section below on manual configuration of a VPN tunnel.

The router will then prompt you to configure the remote ImageStream router, assuming that the RSA signature key was retrieved successfully:

```
The right side router is an ImageSteam router.   Do you want to attempt to configure the right si
```

If you want to attempt to configure the remote router for the VPN tunnel, press 'Y' or leave the entry blank and press **Enter**. If you do not want to configure the remote router, press 'N' and **Enter** and the script will not attempt to automatically configure the remote router.

If you pressed 'Y' or **Enter** the router will then display the following, based on our example:

```
Now creating the tunnel configuration for the right side router...done
Attempting to contact the right side router.   You will be prompted for the password...
Press Control-\ at any time to interrupt the connection process. root@192.168.100.140's password:
```

Enter the password for the remote router and press **Enter**. The script will then upload the proper VPN configuration file to the remote router. The router will then display:

```
ipsec.conf-right        100% |***       *|      1581    00:00
Successfully copied the configuration file to the right side router.

You must start the IPSec service before your configuration will be active.
Remember to save your configuration to flash, or the changes made in the IPSec configuration file

Press enter/return to quit
```

If you have entered 'N' when prompted to configure the remote router, the script will save a copy of the remote configuration and display:

```
A copy of the configuration file for the right side router has been saved in: /tmp/ipsec.conf-rig

You must start the IPSec service before your configuration will be active.
Remember to save your configuration to flash, or the changes made in the IPSec configuration file

Press enter/return to quit
```

If the remote router is an ImageStream router or uses a FreeSwan implementation, you will find a copy of the configuration for that router in the /tmp directory. A copy of the local router's configuration, based on your entries, has been saved on the local router. Using this script does not start the IPSec service, nor will it enable the service on boot. Use the IPSec menu to start or stop IPSec or to enable or disable the service at boot- time.

Note: You must save the settings to the router's non-volatile flash memory! If the router is rebooted before saving, your changes will be lost! See the Chapter 26, "Manual/Backup/Restore Menu: Managing Configurations" for more information.

Selecting manual configuration for a VPN tunnel

If you have entered 'N' when prompted to get the remote router's public RSA key, the router will proceed with manual entry of the VPN tunnel configuration and will display the following, based on our example above:

```
Proceeding with manual entry...
```

```
Please paste the public key from the right side router. Include only the key and NO other characters
When you are finished, press Enter/Return, then press Control-D
```

Enter the public RSA key only with no other special characters or values. The router will automatically remove any line breaks from the input. If you are pasting the public key from another ImageStream router or a FreeSWan implementation, do not include the "pubkey=" when you paste the value. If you are using a standard key, it will look similar to:

```
0sAQNnhVz28e6wHj0IAJzQQiJOTYKfE/+zJbLr86ZbJjfGNMP4gXLm3pf4XFYLCqH
bpYYQoYAq1GJiyTUnXe4k0glELTIqLCoM46U6AwRu9g1hA/NSnHPQD2KF+tlwKGY
G3tD0pu79q6ks+52p7FO8UzdRxUvSYGtP0bs4XQnB1ZeT8g5uyt7ugmlYZh72W5Xe
qR7LCji29h5n2rR64WG385TiNPG60VOmyNHHKzhrR0IDs39hgxezNLW4QeVwb4SX6
/eYZUXGKv2R56R804OTZ0PyzlYQumMzB/KtUBfbwmAKGBAZTY5ODhwQYVL2LrW/Zg
3AAyhkn4lvcEfY8sV316H
```

The key for your routers will be unique and will not match the above example. Press **Enter** and then press **Control-D** when you are finished entering the key. The router will then process your input and display the following, based on our example:

```
Successfully parsed right side public RSA key.
Now creating the tunnel configuration for this router...done
A copy of the configuration file for the right side router has been saved in: /tmp/ipsec.conf-right

You must start the IPSec service before your configuration will be active.
Remember to save your configuration to flash, or the changes made in the IPSec configuration file will b

Press enter/return to quit
```

If the remote router is an ImageStream router or uses a FreeSwan implementation, you will find a copy of the configuration for that router in the /tmp directory. A copy of the local router's configuration, based on your entries, has been saved on the local router. Using this script does not start the IPSec service, nor will it enable the service on boot. Use the IPSec menu to start or stop IPSec or to enable or disable the service at boot-time.

Note: You must save the settings to the router's non-volatile flash memory! If the router is rebooted before saving, your changes will be lost! See the Chapter 26, "Manual/Backup/Restore Menu: Managing Configurations" for more information.

Managing the IPSec Service

Once you have exited the script by pressing Enter, the router will return you to the IPSec menu:

```
     IPSec VPN (Free S/Wan), (stopped)
     1. Configure IPSec (Free S/Wan)
     2. Generate a new Signature Key
     3. Configure a basic IPSec VPN
     4. Enable IPSec on boot
     5. Disable IPSec on boot
     6. Start IPSec
     7. Stop IPSec
     0. Service configuration
```

Enabling IPSec at Boot-time

4. Enable IPSec on boot

Selecting this menu option enables the IPSec service when the router is booted. This does not start the IPSec service on the router if it is not running, unless the router is rebooted first. By default, IPSec is disabled on boot. To enable IPSec at boot-time, select this menu option by pressing 2 and **Enter**. The router will display the following message:

```
ipsec enabled on boot.
```

If IPSec has already been enabled on boot, the router will display the message:

```
ipsec already enabled on boot.
```

The resulting message will only be displayed for a few seconds, and then you will be returned to the SNMP menu.

Disabling IPSec at Boot-time

5. Disable IPSec on boot

Selecting this menu option disables the IPSec service when the router is booted. This does not stop the IPSec service if it is running, unless the router is rebooted first. To disable IPSec on boot, select this menu option by pressing 3 and **Enter**. The router will display the following message:

```
ipsec disabled on boot.
```

If IPSec has already been disabled on boot, the router will display the message:

```
ipsec already disabled on boot.
```

The resulting message will only be displayed for a few seconds, and then you will be returned to the IPSec menu.

Starting the IPSec Service

6. Start IPSec

Selecting this menu option starts the IPSec service on the router. Starting IPSec does not automatically enable the IPSec service when the router is booted. To start the IPSec service, select this menu option by pressing 4 and **Enter**. The router will display the following message:

```
Starting ipsec...done.
```

The message will only be displayed for a few seconds, and then you will be returned to the IPSEc menu.

Stopping the IPSec Service

7. Stopping IPSec

Selecting this menu option stops the IPSec service on the router. Stopping IPSec does not automatically disable the IPSec service when the router is booted. To stop the IPSec service, select this menu option by pressing 5 and **Enter**. The router will display the following message:

```
Stopping ipsec...done.
```

The message will only be displayed for a few seconds, and then you will be returned to the IPSec menu.

Returning to the Service Configuration Menu

0. Service configuration

Selecting this menu option returns you to the "Service configuration" menu. To return to the Service configuration menu, press 0 and **Enter**. The router will display the Service configuration menu:

```
Service configuration
1. System scheduler (cron), (running)
2. Dialout PPP, (stopped)
3. IPSec VPN (Free S/Wan), (stopped)
4. NetFlow exporter (nprobe), (stopped)
5. network interfaces (sand), (running)
6. sconsole (mgetty), (running)
7. snmp (net-snmp), (stopped)
8. ssh (OpenSSH), (running)
0. Configuration menu
```

Changes for 4.4

The 4.4 release uses a newer version of OpenSwan with the kernel 2.6 native transform implementation for IPSec.
Use ipsec setup --status to check on tunnel establishment and ip xfrm policy and ip xfrm state to check on transforms.
The ipsec.conf configuration file will need some changes when upgrading from 4.2 to 4.4.

◊ Add **version 2** above config setup line.

◊ Change interfaces="ipsec0=xxx" to interfaces="%defaultroute" as we don't use klips anymore so there is no ipsec0 interface.

◊ Remove **plutostart** and **plutoload** commands from the config setup because they've been deprecated.

◊ Be sure to add authby=secret in sections where it isn't specified unless you have it in a default section since this is no longer the default authorization mode.

◊ Check NAT rules to ensure you're not nat'ing traffic that should be IPSec transformed. The 4.2 release used an ipsec0 interface but the 2.6 kernel adds routes via the normal default gateway so it is possible that your nat rules will start matching traffic under 4.4 that they didn't match under 4.2. The easiest solution is to add accept rules for the IPSec subnets above the SNAT rules.

Version 4.2 ipsec.conf:

```
config setup
        interfaces="ipsec0=Ethernet0"
        klipsdebug=none
        plutodebug=none
        plutostart=%search
        plutoload=%search
        uniqueids=yes
        plutowait=no
```

Version 4.4 ipsec.conf:

```
version 2
config setup
        interfaces="%defaultroute"
        klipsdebug=none
        plutodebug=none
        uniqueids=yes
        plutowait=no
```