# VPN Connection to D-Link DI-804V Router

1 November 2002

This document explains how to configure a virtual private network connection over an open network from a remote host running SSH Sentinel to a private network protected by a D-Link DI-804V router acting as a security gateway.

**SSH Communications Security Corp.**
Fredrikinkatu 42
FIN-00100 Helsinki
FINLAND

SSH Communications Security Inc.
1076 East Meadow Circle
Palo Alto, CA 94303
USA

SSH Communications Security K.K.
House Hamamatsu-cho Bldg. 5F
2-7-1 Hamamatsu-cho, Minato-ku
Tokyo 105-0013, JAPAN

http://www.ssh.com/
e-mail: ipsec-sales@ssh.com (sales), sentinel-support@ssh.com (technical support)
Tel: +358 20 500 7030 (Finland), +1 650 251 2700 (USA), +81 3 3459 6830 (Japan)
Fax: +358 20 500 7031 (Finland), +1 650 251 2701 (USA), +81 3 3459 6825 (Japan)

# Contents



 

# Chapter 1

# VPN Connection to D-Link DI-804V Router

## 1.1 Introduction

This document contains all the required information for setting up a D-Link DI-804V router to accept connections from SSH Sentinel VPN clients. A pre-shared key is used for authentication.

**Note:** For documentation on how to configure firewall, NAT, DHCP or other such features of DI-804V, refer to the D-Link documentation.

### 1.1.1 Further Information

- SSH Sentinel User Manual
- SSH Sentinel support: `http://www.ipsec.com`
- D-Link Systems, Inc: `http://www.d-link.com`

### 1.1.2 Platform Requirements

The interoperability between SSH Sentinel and D-Link DI-804V is tested using the following components:

- SSH Sentinel VPN client v1.4
- D-Link DI-804V router, firmware C4.73

 

## 1.2 Configuring D-Link DI-804V

### 1.2.1 Open Management Interface

By default, your manage the D-Link DI-804V router with a Web interface found in the URL http://192.168.0.1. Refer to the D-Link documentation for your user account and password.

Configure your DI-804V settings (for example, the LAN and WAN settings) according to the instructions in the D-Link documentation.

### 1.2.2 Create a VPN Tunnel for Roadwarriors

In this setup, the gateway accepts connections from any IP address. All clients use the same shared secret for authentication.

1. In the main menu, Click **VPN Settings** to open the VPN configuration form.

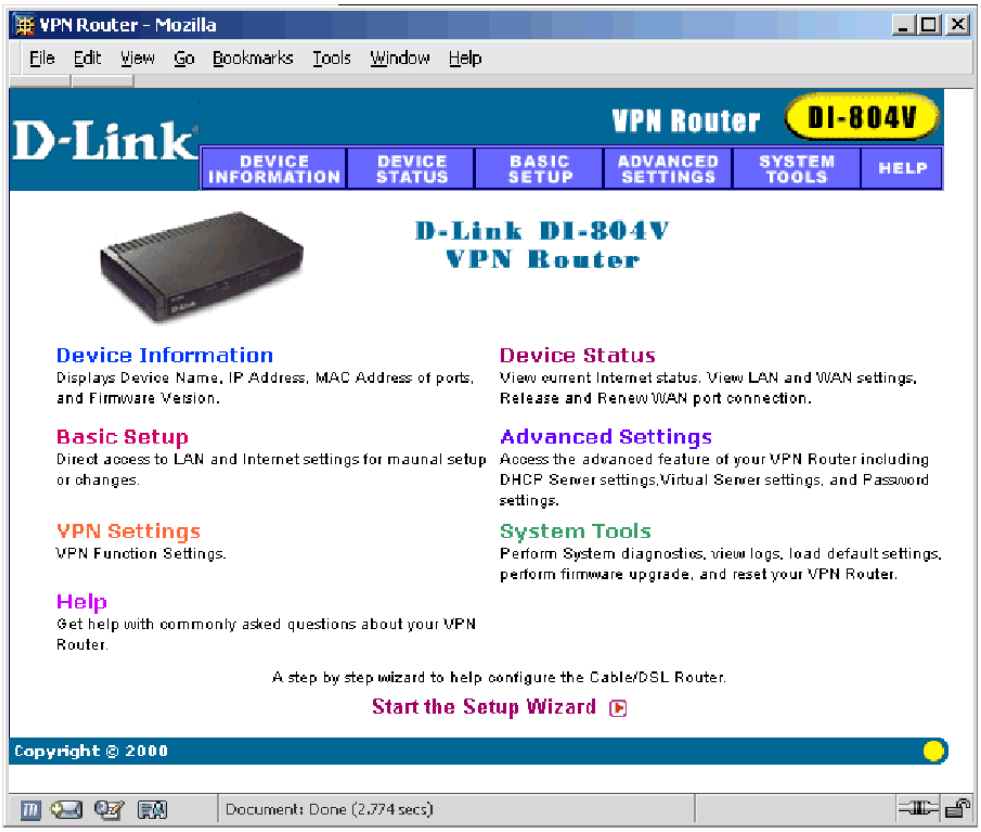


Figure 1.1: Main menu

2. Click **Basic Setup** and create a new VPN tunnel as shown in Figure 1.2 (Basic setup):

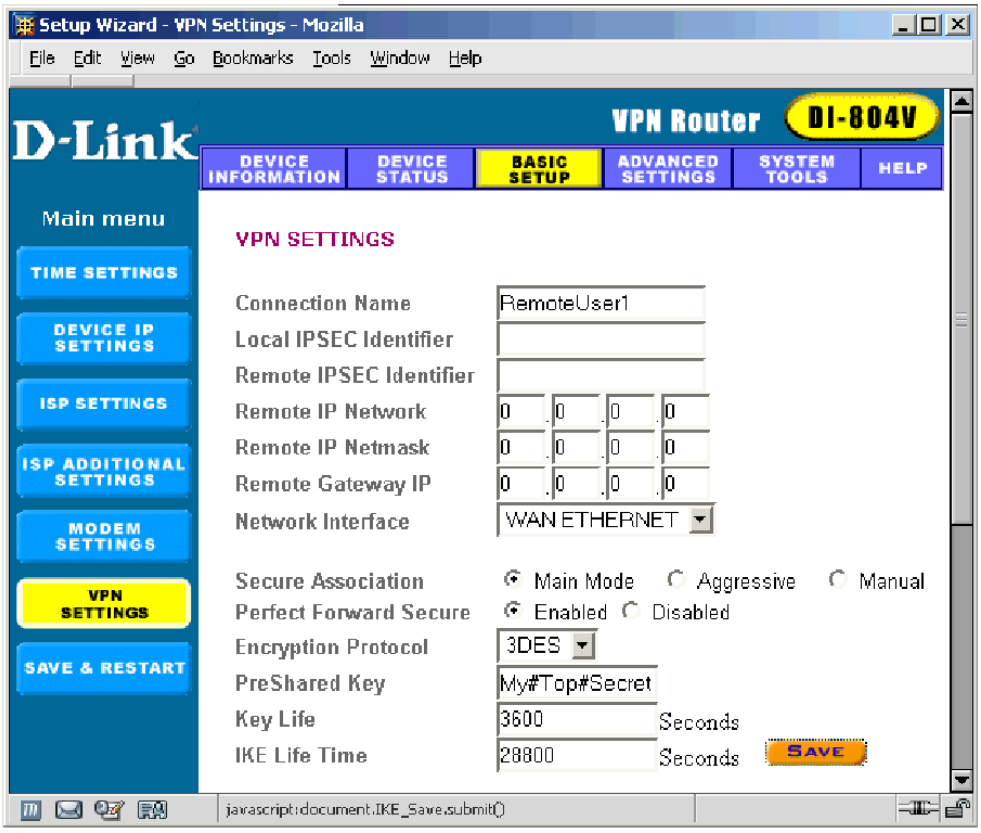


Figure 1.2: Basic setup

3. Save the settings and restart the gateway with **Save & Restart**.

**Note:** From the general security point of view, sharing a single secret with all the users is not recommended. To create separate tunnels for each remote user, create separate shared secrets.

## 1.3 Configuring SSH Sentinel

### 1.3.1 Create the Pre-Shared Key

On the **Key Management** page of the Policy Editor, select **My Keys** and click **Add** to create a new pre-shared key. For detailed instructions, see the SSH Sentinel User Manual.

In this example, the following values are used:

- Name: MyDLinkPSK
- Shared secret: My#Top#Secret

 

### 1.3.2 Create the VPN Rule

1. On the **Security Policy** page of the Policy Editor, select **VPN Connections** and click **Add** to create a new VPN connection rule. For detailed instructions, see the SSH Sentinel User Manual. Specify the following values (see Figure 1.3 (The general properties of the VPN connection)):

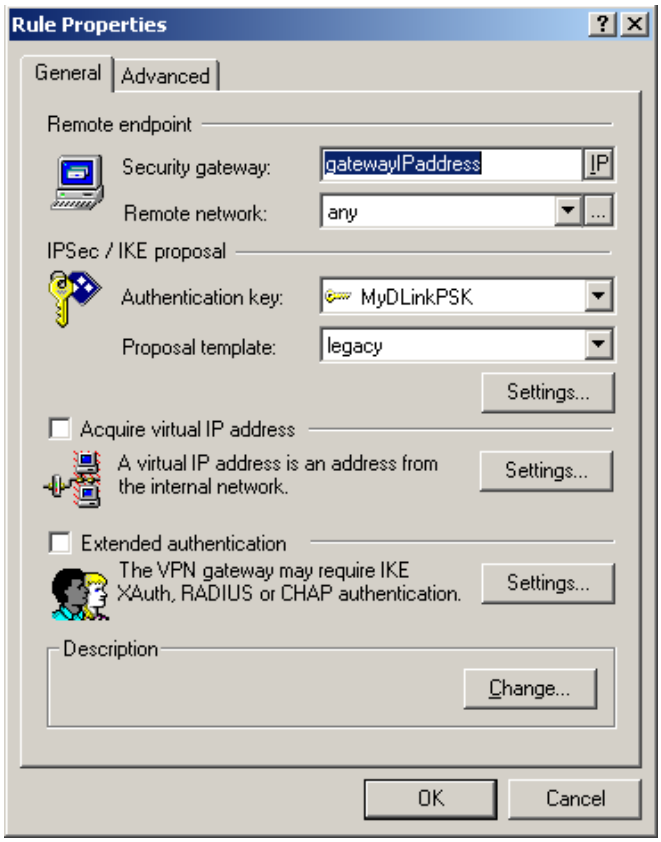


Figure 1.3: The general properties of the VPN connection

- Security gateway: *the IP address of the gateway*
- Remote network: any (0.0.0.0/0)
- Authentication key: MyDLinkPSK
- Proposal template: legacy

2. On the **Rule properties** dialog box, under **IPSec/IKE proposal**, click **Settings** to specify the following:

   - IKE proposal
     - Encryption algorithm: 3DES
     - Integrity function: MD5
     - IKE mode: main mode
     - IKE group: MODP 1024 (group 2)

- IPSec proposal
  - Encryption algorithm: 3DES
  - Integrity function: HMAC-MD5
  - IPSec mode: tunnel
  - PFS group: MODP 1024 (group 2)

3. On the **Advanced** page, the default values for **Security Association Lifetimes** should be OK.

   In addition, select the options **Audit this rule**, **Discover path maximum transfer unit (PMTU)**, and **Deny split tunneling**.

4. Click **OK** and **Apply** to save the settings.

5. Select the D-Link VPN rule and click **Diagnostics** to probe the connection.

6. Open the VPN tunnel via the SSH Sentinel tray icon.

7. Ping the private interface of the router and verify that traffic goes through the VPN tunnel.

## 1.4 Troubleshooting

The audit logs and IKE log are available in SSH Sentinel for troubleshooting. Refer to the SSH Sentinel User Manual for details.

 