VPN Connection to Linksys BEFVP41

2 December 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 Linksys BEFVP41 VPN 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 Linksys BEFVP41 Gateway

1.1 Introduction

This document contains all the required information for setting up a Linksys BEFVP41 gateway to accept connections from SSH Sentinel 1.4 VPN clients. Linksys BEFVP41 is a popular light VPN device. The moderate price and the large set of features makes it suitable for SOHO use.

Note: For documentation on how to configure firewall, NAT, DHCP, or other such features of the device, refer to the Linksys documentation.

1.1.1 Further Information

- SSH Sentinel User Manual
- SSH Sentinel support: `http://www.ipsec.com`
- Linksys Inc: `http://www.linksys.com`

1.1.2 Platform Requirements

The interoperability between SSH Sentinel and Linksys BEFVP41 is tested using the following components:

- SSH Sentinel VPN client v1.4
- Linksys BEFVP41 VPN router, firmware v1.40.4

The firmware of Linksys BEFVP41 is available on Linksys Web site and a local administrator can upgrade it easily. The instructions on how to do this are also available on the Web site.

Note: These instructions are also applicable to Linksys BEFSX41 gateway. The tested version is Linksys BEFSX41 VPN router, firmware v1.44.

Linksys BEFVP41 can handle up to 70 simultaneous IPSec VPN tunnels, whereas Linksys BEFSX41 can handle up to two simultaneous tunnels. See the Linksys Web site for more information.

1.2 Configuring Linksys BEFVP41

By default, your manage the Linksys BEFVP41 gateway with a Web interface found in the URL `http://192.168.1.1`. Refer to the Linksys documentation for your user account and password.

1.2.1 Create a New VPN Tunnel

Click **VPN** to open the VPN configuration form. Create a new VPN tunnel as follows:

- This tunnel: enable
- Tunnel name: SentinelUser01
- Local source group
  - Subnet IP: 192.168.1.0
  - Mask: 255.255.255.0
- Remote secure group: Any
- Remote security gateway: Any
- Encryption: 3DES
- Authentication: MD5
- Key management: Auto (IKE)
- Select the option **PFS** (Perfect Forward Secrecy)
- Pre-shared key: MyVerySecretPSK
- Key lifetime: 3600 sec

The following settings are found in the **More** submenu:

Phase 1:

- Operation mode: Main mode
- Proposal 1:
  - Encryption: 3DES
  - Authentication: MD5
  - Group: 1024-bit
  - Key lifetime: 14400 Sec

Phase 2, proposal:

- Encryption: 3DES
- Authentication: MD5
- Group: 1024-bit
- Key lifetime: 3600 Sec

Other options: *clear all*

Click **Apply** to save the changes.

Note: The created VPN rule accepts connections from any IP address. 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: MyLinksysPSK
- Shared secret: MyVerySecretPSK

1.3.2 Create the VPN Rule

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:

- Security gateway: *the IP address of the gateway*
- Remote network: 192.168.1.0/255.255.255.0
- Authentication key: MyLinksysPSK
- Proposal template: legacy.

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)

If running firmware v1.40.2 or older on the gateway, select the option **Attach only the selected values to the proposal**.

Click **Settings** on the **Advanced** page to specify the following settings:

- Security association lifetimes / IKE
  - Lifetime in minutes: 240 min
  - Lifetime in megabytes: 0 MB
- Security association lifetimes / IPSec
  - Lifetime in minutes: 60 min
  - Lifetime in megabytes: 400 MB

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

Note: If you select the option **Open on start-up**, the VPN connection is automatically opened after a system reboot or SSH Sentinel Policy Manager restart. You can naturally also open the connection manually from the SSH Sentinel tray icon. Refer to SSH Sentinel User Manual for detailed information.

1.3.3 Set a Virtual IP Address Manually

In most cases, the basic VPN settings explained above should be enough. However, if you wish to use virtual IP addressing, you can set a virtual IP address manually for the client.

Setting the virtual IP address manually requires that the administrator takes care of the IP addressing to prevent IP conflicts (whereas the L2TP, DHCP over IPSec, and IKE Config Mode protocols take care of assigning the virtual IP address to the host themselves).

To set a virtual IP address manually after successfully setting up the system, you do not have to make any additional settings for your Linksys BEFVP41 gateway. The following SSH Sentinel settings are required:

1. On the **Security Policy** page of the Policy Editor, select the Linksys connection and click **Properties**.
2. Select the check box **Acquire virtual IP address**, click **Settings...**, and select **Specify manually**.
3. By default Linksys uses 192.168.1.0/24 for private LAN IP addressing. Try using 192.168.2.0/24 for remote clients. Enter any IP address from the subnet (for example, 192.168.2.1/255.255.255.0) for the virtual IP address of the first remote client. Select the next available IP address for the next remote client, and so on.
4. Enter the DNS and WINS server IP addresses for the VPN rule.

   When the VPN tunnel is active, the SSH Sentinel client uses these nameservers for DNS and WINS queries. For example, if you have a Dynamic DNS (DDNS) server in your target private LAN taking care of the DNS for a MS Windows 2000 Active Directory based domain, your SSH Sentinel remote client will now be able to use that private DDNS server over the VPN tunnel. The same works for WINS server usage if your private target LANS still prefers NetBIOS over TCP/IP and an older MS Windows domain model (like the MS Windows NT 4.0 domain).

About the Routing in the Private LAN

If Linksys is the default gateway for the private LAN, the above settings are enough.

If the default gateway is something else (such as a Cisco gateway or another Linksys gateway), and you are creating a VPN tunnel from SSH Sentinel via this secondary gateway to your private LAN using manual virtual IP addressing, you have to add a static route into your default gateway device to route the virtual IP subnet (192.168.2.0/24 in the example above) to the private interface of your Linksys BEFVP41 gateway.

1.4 Troubleshooting

To increase the debugging level in Linksys BEFVP41 v1.40.4 gateway, browse to the URL `http://192.168.1.1/LogManage.htm` (not documented) on the Linksys management Web server. Select both **Access log** and **System log** for enhanced debugging.

To view the VPN log, open the page `http://192.168.1.1/VPNLog.htm`.

Different firmware versions may have different URLs.

After having solved the problem, it is recommended that you revert to a lower debugging level. Exhaustive logging may slow down the performance of the gateway.

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