



## VPN Connection to SonicWALL TELE3 Gateway

---

28 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 SonicWALL TELE3 gateway.

© 2000-2002 SSH Communications Security Corp

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of SSH Communications Security Corp.

This software is protected by international copyright laws. All rights reserved. ssh® is a registered trademark of SSH Communications Security Corp in the United States and in certain other jurisdictions. SSH2, the SSH logo, IPSEC Express, SSH Certifier, SSH Sentinel, SSH NAT Traversal, IPSEC on silicon, Hypermode, SSH Accession, SSH Token Master, SSH Secure Shell and Making the Internet Secure are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

**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](mailto:ipsec-sales@ssh.com) (sales), [sentinel-support@ssh.com](mailto: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

<b>1</b>	<b>VPN Connection to SonicWALL VPN Gateway</b>	<b>5</b>
1.1	Environment . . . . .	5
1.1.1	Further Information . . . . .	5
1.2	Configuring SonicWALL VPN Gateway . . . . .	6
1.3	Configuring SSH Sentinel . . . . .	7
1.3.1	Setting a Virtual IP Address Manually . . . . .	7



## Chapter 1

# VPN Connection to SonicWALL VPN Gateway

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 SonicWALL VPN gateway.

### 1.1 Environment

The SonicWALL VPN gateway acts as a security gateway that protects the private network and filters out unauthorized network traffic from and to the open network. SSH Sentinel runs on the remote host that contacts the SonicWALL VPN gateway in order to access the private network.

The SSH Sentinel version used in the sample configuration is SSH Sentinel 1.4. The SonicWALL gateway used is SonicWALL TELE3, firmware v6.3.1.4.

A pre-shared key is used as the authentication method in the configuration.

#### 1.1.1 Further Information

- SSH Sentinel 1.4 User Manual
- SSH Sentinel support: <http://www.ipsec.com>
- SonicWALL Inc: <http://www.sonicwall.com>

## 1.2 Configuring SonicWALL VPN Gateway

The necessary settings of the SonicWALL VPN gateway are shown in Figure 1.1 (The general properties of the VPN connection I). In addition, make sure to enable perfect forward secrecy on the Advanced Settings page (see Figure 1.2 (The advanced settings)).

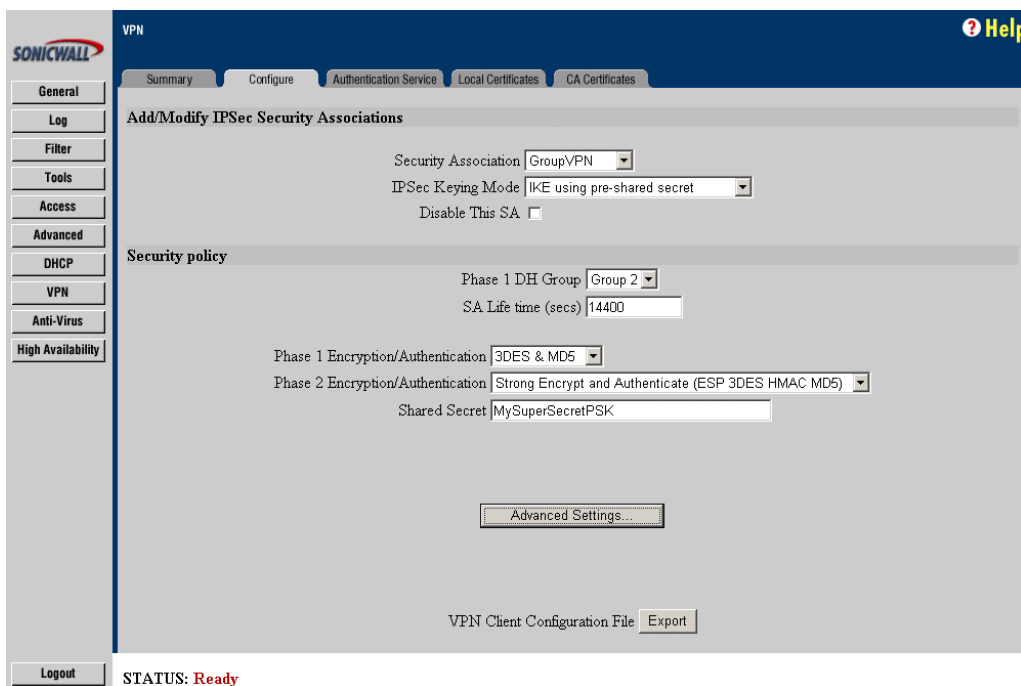


Figure 1.1: The general properties of the VPN connection I

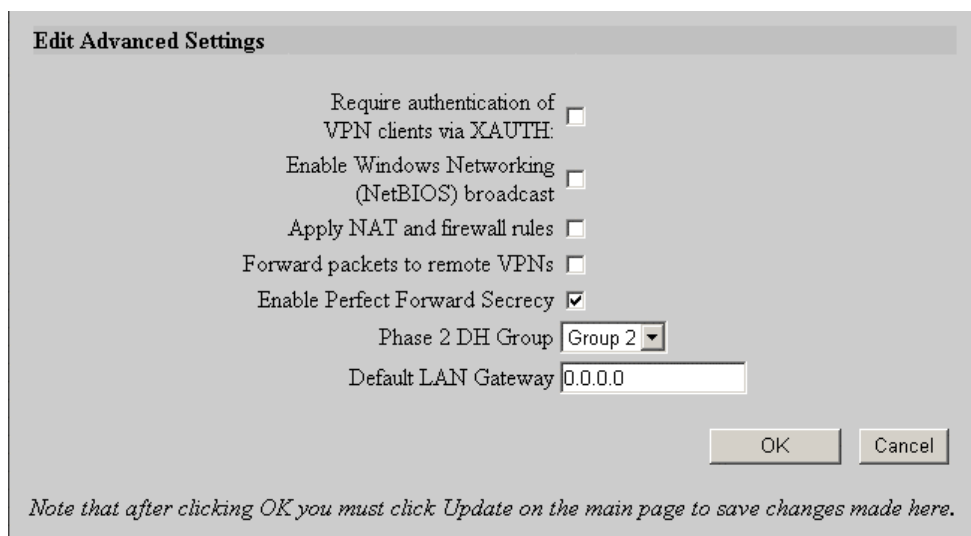


Figure 1.2: The advanced settings

## 1.3 Configuring SSH Sentinel

In SSH Sentinel, do the following:

1. On the **Key Management** page of the Policy Editor, create the appropriate pre-shared key. The actual key must naturally be the same as defined in the SonicWALL gateway.
2. On the **Security Policy** page of the Policy Editor, select **VPN Connections** and click **Add** to create a new virtual private network connection rule with the following information (see Figure 1.3 (The general properties of the VPN connection II), replace the IP addresses with the correct values):
  - Security gateway: The external IP address of the gateway.
  - Remote network: The IP address and netmask of the internal network.
  - Authentication key: The pre-shared key you created in the previous step.
  - Proposal template: Legacy proposal.

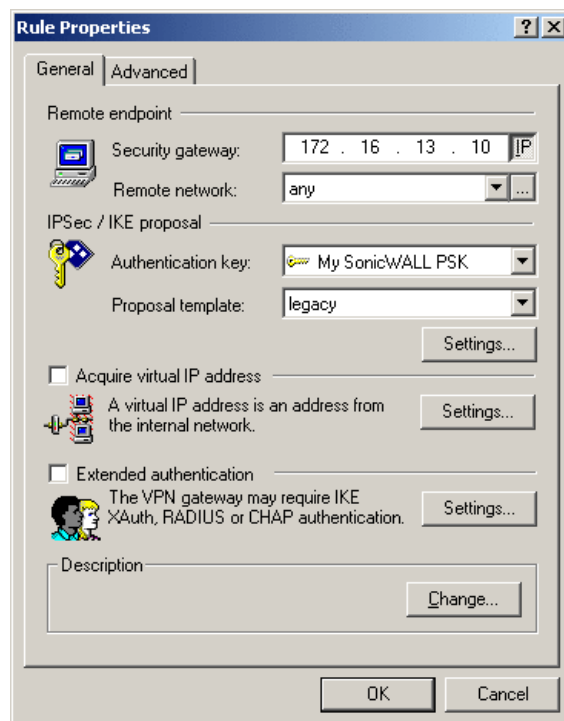


Figure 1.3: The general properties of the VPN connection II

### 1.3.1 Setting 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 SonicWALL gateway. The following SSH Sentinel settings are required:

1. On the **Security Policy** page of the Policy Editor, select the SonicWALL connection and click **Properties**.
2. Select the check box **Acquire virtual IP address**, click **Settings...**, and select **Specify manually**.
3. If 192.168.1.0/24 is used 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 SonicWALL 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 SonicWALL 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 SonicWALL gateway.