



VPN Connection to ZyXEL ZyWALL VPN Gateway

17 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 ZyXEL ZyWALL VPN 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 (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

1	VPN Connection to ZyXEL ZyWALL VPN Gateway	5
1.1	Introduction	5
1.1.1	Further Information	6
1.1.2	Platform Requirements	6
1.2	Configuring ZyXEL ZyWALL VPN Gateway	6
1.3	Configuring SSH Sentinel	7
1.3.1	Create the Pre-Shared Key	8
1.3.2	Create the VPN Rule	8
1.4	Troubleshooting	9

Chapter 1

VPN Connection to ZyXEL ZyWALL VPN Gateway

1.1 Introduction

This document instructs configuring a ZyXEL ZyWALL series VPN gateway for a roadwarrior VPN gateway usage and setting up SSH Sentinel VPN client to connect to the target private LAN over the gateway.

Note: For documentation on how to configure other features of ZyXEL ZyWALL, please refer to the ZyXEL ZyWALL manuals available at <http://www.zywall.com/>.

The following proposal settings are used in the example configuration:

- Authentication: Pre-shared key
- IKE Encryption: 3DES
- IKE Integrity: MD5
- IKE Mode: Main mode
- IKE Group: MOPD 1024 (group 2)
- IPSec Encryption: 3DES
- IPSec Integrity: HMAC-MD5
- IPSec Mode: Tunnel
- PFS Group: MODP 1024 (group 2)

Note: Virtual IP addressing (DHCP over IPSec, L2TP, manually assigned virtual IP address) and extended authentication (XAuth) techniques are not supported by the gateway. For more information, please consult ZyXEL support.

1.1.1 Further Information

- SSH Sentinel User Manual
- SSH Sentinel support: <http://www.ssh.com>
- ZyXEL Communications Corp: <http://www.zywall.com>

1.1.2 Platform Requirements

The interoperability between SSH Sentinel and ZyXEL ZyWALL was tested with the following components:

- SSH Sentinel VPN client 1.4
- ZyXEL ZyWALL 50 VPN gateway, firmware V3.50(WC.3) 17 June 2002

1.2 Configuring ZyXEL ZyWALL VPN Gateway

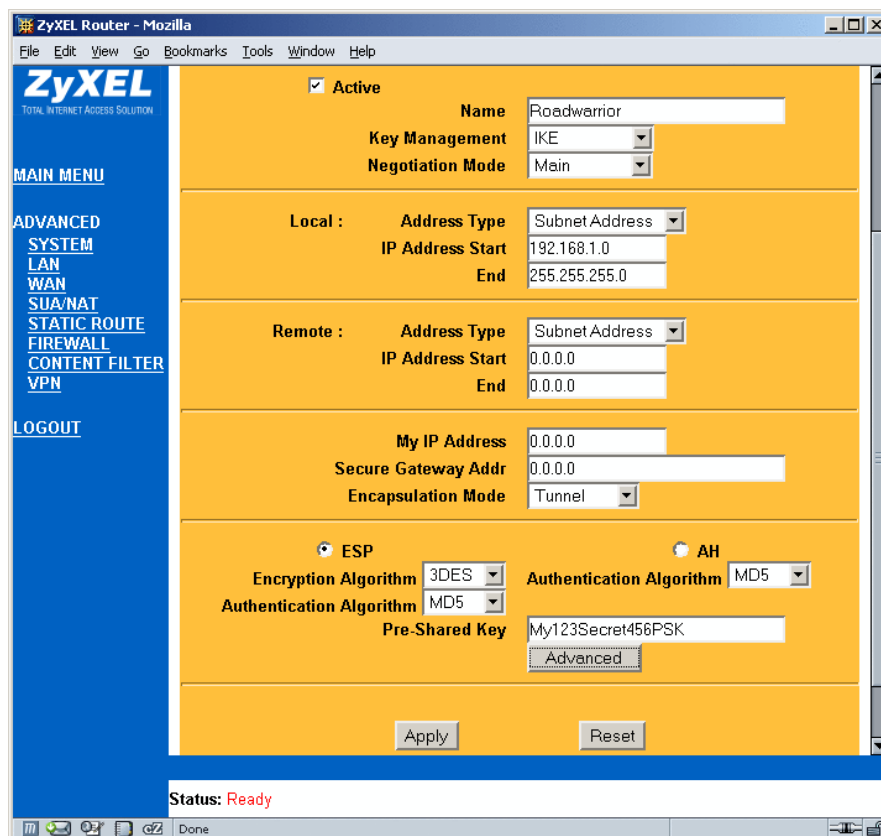


Figure 1.1: VPN rule

1. To declare a VPN tunnel, launch the ZyXEL Web Configurator at `http://192.168.1.1`.
2. Using the Web Configurator, configure IP addresses for the WAN and LAN interfaces as instructed in the ZyWALL user manual. This document assumes that you keep the factory default IP address (192.168.1.1, netmask 255.255.255.0) for the LAN interface. Your private LAN is then 192.168.1.0/255.255.255.0 (equals to 192.168.1.0/24).
3. To configure a roadwarrior VPN profile, Click **Advanced** → **VPN** (see Figure 1.1 (VPN rule)).
4. Click the **Advanced** button to set IKE Phase 1 and Phase 2 parameters (see Figure 1.2 (IKE Phase 1 and Phase 2 parameters)).

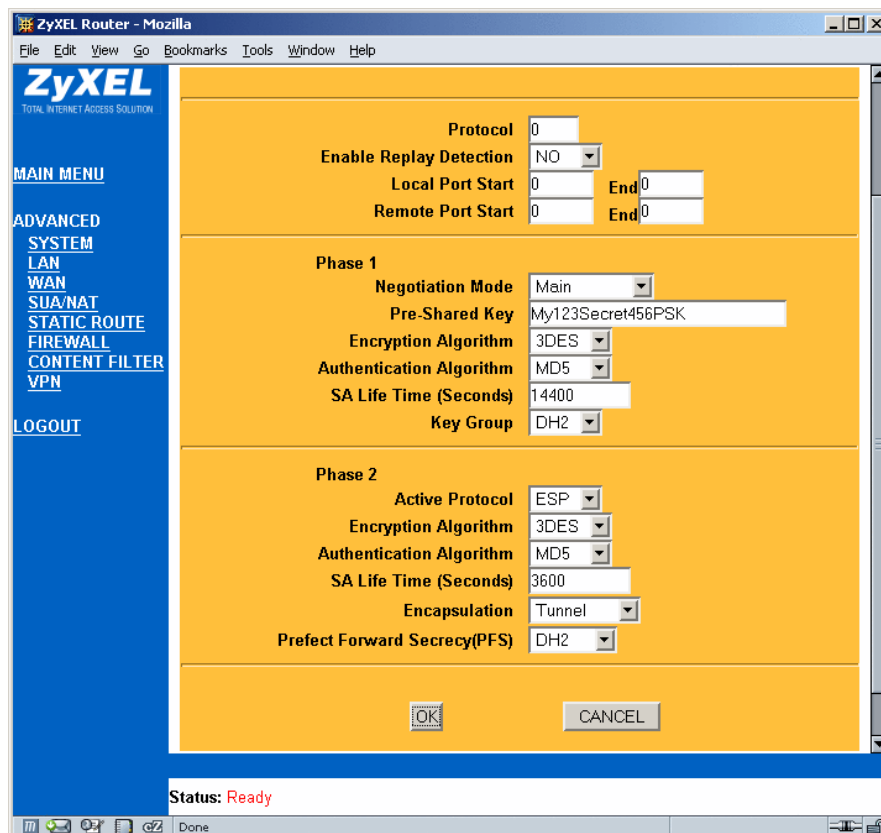


Figure 1.2: IKE Phase 1 and Phase 2 parameters

1.3 Configuring SSH Sentinel

On the SSH Sentinel side, you need to do two things: Create a pre-shared key to be used for authentication, and create a connection rule to control the data traffic from the SSH Sentinel host to the private network via the ZyXEL ZyWALL VPN gateway. For basic information on how to create pre-shared keys and connection rules, see the appropriate sections in the SSH Sentinel User Manual.

1.3.1 Create the Pre-Shared Key

First, create the pre-shared key needed for authentication. On the **Key Management** page of the Policy Editor, select **My Keys** and click **Add** to create a new pre-shared key. Remember to click **Apply** to update the settings.

For detailed instructions, see the SSH Sentinel User Manual.

1.3.2 Create the VPN Rule

1. On the **Security Policy** page of the Policy Editor, select **VPN Connections** and click **Add** to add a new VPN rule. Specify the following values (see Figure 1.3 (The general properties of the VPN connection)):

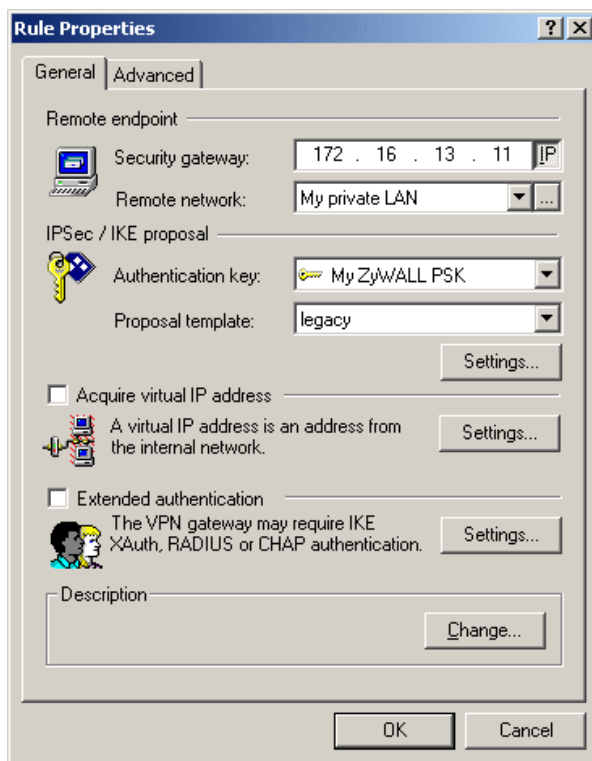


Figure 1.3: The general properties of the VPN connection

- **Security gateway:** The IP address of the ZyXEL ZyWALL (in this example, 172.16.13.11), or a Fully Qualified Domain Name (FQDN) of the public WAN interface of the ZyXEL ZyWALL VPN gateway.

Note: If the WAN interface has a dynamic IP address, you may want to use the DDNS capabilities of the ZyXEL ZyWALL gateway. Your ZyWALL has DNNS client features, and it can update a dynamic DNS entry at your DDNS vendor (for example, <http://www.dyndns.org>). Even if the dynamic IP address is changed by an ISP DHCP server, your VPN gateway can always be

reached using the FQDN that your ZyXEL ZyWALL VPN gateway keeps automatically up-to-date.

For more information, please check the ZyXEL ZyWALL documentation and your DNS service information.

- **Remote network:** Using the **Network Editor** (click the ... button on the right to open the editor), declare a remote network profile for your LAN. In this example, the profile name is `My Private LAN` and the network is `192.168.1.0/255.255.255.0`.
 - **Authentication key:** Select the pre-shared key that you created earlier.
 - **Proposal template:** Legacy proposal.
2. On the **Rule Properties** dialog box, under **IPSec/IKE proposal**, click **Settings** to specify the following settings:
- **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)

Note: Verify that the proposal settings match those used by your ZyWALL VPN profile.

1.4 Troubleshooting

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