



VPN Connection to MultiTech RF550VPN

8 October 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 MultiTech RF550VPN 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 Multi-Tech RF550VPN Gateway	5
1.1	Introduction	5
1.1.1	Further Information	5
1.1.2	Platform Requirements	5
1.2	Configuring Multi-Tech RF550VPN	6
1.2.1	Open Management Interface	6
1.2.2	Create a VPN Tunnel for Roadwarriors	6
1.2.3	Create a VPN Tunnel for a Remote Client with Fixed IP Address	7
1.3	Configuring SSH Sentinel	7
1.3.1	Create the Pre-Shared Key	7
1.3.2	Create the VPN Rule	8
1.4	Troubleshooting	9

Chapter 1

VPN Connection to Multi-Tech RF550VPN Gateway

1.1 Introduction

This document contains all the required information for setting up a Multi-Tech RF550VPN gateway to accept connections from SSH Sentinel v1.3 VPN clients. Multi-Tech RF550VPN is a popular cost-effective 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 Multi-Tech RF550VPN, refer to the Multi-Tech documentation.

1.1.1 Further Information

- SSH Sentinel 1.4 User Manual
- SSH Sentinel support: <http://www.ipsec.com>
- Multi-Tech Systems, Inc: <http://www.multitech.com>

1.1.2 Platform Requirements

The interoperability between SSH Sentinel and Multi-Tech RF550VPN is tested using the following components:

- SSH Sentinel VPN client v1.4
- Multi-Tech RF550VPN VPN router, firmware v4.62

The firmware of Multi-Tech RF550VPN is available on Multi-Tech Website and a local administrator can upgrade it easily. The instructions on how to do this are also available on the Website.

1.2 Configuring Multi-Tech RF550VPN

1.2.1 Open Management Interface

By default, you manage the Multi-Tech RF550VPN gateway with a Web interface found in the URL <http://192.168.2.1>. Refer to the Multi-Tech documentation for your user account and password.

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. Multi-Tech RF550VPN supports only authentication with pre-shared keys.

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

- Connection name: Roadwarrior
- Select the option **Disable UID**
- Local IPSec identifier: *empty*
- Remote IPSec identifier: *empty*
- Remote IP network: 0.0.0.0
- Remote IP netmask: 0.0.0.0
- Remote gateway IP: 0.0.0.0
- Network interface: WAN ETHERNET
- Secure association: IKE
- Perfect Forward Secure: Enabled
- Encryption protocol: 3DES
- Pre-shared key: VerySecretPSKforRoadwarriors
- Key lifetime: 3600 seconds
- IKE lifetime: 28800 seconds

Save the settings and restart the gateway with **SaveRestart**.

Note: From the general security point of view, sharing a single secret with all the users is not recommended.

1.2.3 Create a VPN Tunnel for a Remote Client with Fixed IP Address

Click **VPN Settings** to open the VPN configuration form. Create a VPN tunnel for a remote user with an IP address 172.16.8.4 as follows:

- Connection name: SentinelUser01
- Select the option **Disable UID**
- Local IPSec identifier: *empty*
- Remote IPSec identifier: *empty*
- Remote IP network: 172.16.8.4
- Remote IP netmask: 255.255.255.255
- Remote gateway IP: 172.16.8.4
- Network interface: WAN ETHERNET
- Secure association: IKE
- Perfect Forward Secure: Enabled
- Encryption protocol: 3DES
- Pre-shared key: VerySecretPSKforUser01
- Key lifetime: 3600 seconds
- IKE lifetime: 28800 seconds

Save the settings and restart the gateway with **SaveRestart**.

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 the roadwarrior example, the following values are used:

- Name: MyMultiTechPSK
- Shared secret: VerySecretPSKforRoadwarriors

In the example with fixed IP addresses, the following values are used:

- Name: MyMultiTechPSK
- Shared secret: VerySecretPSKforUser01

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: 192.168.2.0/255.255.255.0
- Authentication key: MyMultiTechPSK
- 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)

Furthermore, 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.

1.4 Troubleshooting

To check the status of the current VPN connections to the gateway and to view the VPN log, browse to the URL <http://192.168.2.1>. Click first **Device status** and then either **VPN Status** or **VPN Log**.

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