



VPN Connection to Check Point VPN Gateway

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 Check Point 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 Check Point VPN-1	5
1.1	Environment	5
1.2	Configuring Check Point VPN-1	5
1.3	Configuring SSH Sentinel	6
1.3.1	Authentication	6
1.3.2	Connection Rule	6

Chapter 1

VPN Connection to Check Point VPN-1

This document explains how to configure a virtual private network connection over an open network (the Internet) from a remote host running SSH Sentinel to a private network protected by a Check Point VPN-1.

1.1 Environment

In the test environment the Check Point VPN and FireWall-1 v4.1 SP2 software were running on Nokia VPN-210 hardware. The SSH Sentinel version is 1.4.

1.2 Configuring Check Point VPN-1

In the Check Point end, create a new rule to control the data traffic between the Sentinel host (source) and the private network (destination). When creating the workstation object for the Sentinel host, pay special attention to the following settings on the general page:

Location

Internal or external.

Type

Host

And on the VPN page:

Select IKE and click button to edit the values.

Key Negotiation Encryption Method(s)

DES, CAST, 3DES

Hash Method

MD5, SHA1

Authentication Method

Select **Pre-Shared secret** and click **Edit Secrets** to type the secret. Naturally, the secret must be the same in Sentinel and Check Point.

Supports Aggressive Mode

Yes or No

Supports Subnets

Yes

1.3 Configuring SSH Sentinel

On the SSH Sentinel side, you need to do two things: Create a pre-shared secret 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 Check Point firewall router. 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 Authentication

First create the pre-shared key needed for authentication. Needless to say, the actual secret must be the same in both ends.

1.3.2 Connection Rule

Create the appropriate VPN (virtual private network) connection rule with the following settings:

- Security gateway: The IP address of the Check Point firewall.
- Authentication key: Select the pre-shared key that you created in the previous step.
- IKE and SA lifetimes: Use the default values