



VPN Connection to Cisco PIX Router

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 Cisco PIX router acting as a security 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 Cisco PIX Router	5
1.1	Environment	5
1.2	Configuring Cisco PIX	5
1.3	Configuring SSH Sentinel	7

Chapter 1

VPN Connection to Cisco PIX Router

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 Cisco PIX router acting as a security gateway.

1.1 Environment

In this exemplary network environment, the Cisco PIX router 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 Cisco PIX security gateway in order to access the private network.

The Cisco PIX version tested is 5.3. The configuration is most likely applicable to other versions, too, but it is not guaranteed. Check the Cisco Website for more instructions. The SSH Sentinel version used in the sample configuration is Sentinel 1.4.

For authentication, a pre-shared key is used.

For further information on configuring Cisco PIX routers, refer to the Cisco PIX manuals available on Cisco's Web site (<http://www.cisco.com/univercd/cc/td/doc/product/software/>).

1.2 Configuring Cisco PIX

In the following, the IKE and IPSec settings are specified.

```
# The settings for IKE negotiation
# The hash function can alternatively be set to sha instead of md5.
# The security association lifetimes are set to 14400, the default
```

```

# value in SSH Sentinel.
# SECRET is the pre-shared secret used when communicating with
# the host in IP address 192.168.5.10
isakmp policy 10
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 authentication pre-share
isakmp policy 10 group 2
isakmp policy 10 lifetime 14400
isakmp key SECRET address 192.168.5.10

# Create an access list to define the traffic to be controlled.
# In this case the traffic from the public network 192.168.5.0/24
# to the private network 10.2.1.0/24 is controlled.
# The name of the list is arbitrary.
access-list ACLtest permit 192.168.5.0 255.255.255.0 10.2.1.0
                                                255.255.255.0

# The IPsec transformations
crypto ipsec transform-set TestSet esp-des esp-sha-hmac

# The crypto map is defined next
# Security association lifetimes are set to the default values of
# SSH Sentinel
crypto map TestMap 10 ipsec-isakmp
crypto map TestMap 10 match address ACLtest
crypto map TestMap 10 set transform-set TestSet
crypto map TestMap 10 set security-association lifetime seconds 3600
crypto map TestMap 10 set security-association lifetime kilobytes 400000

# The crypto map has to be applied to an interface (normally outside)
crypto map TestMap interface outside

# Specify that IPsec traffic is implicitly permitted
sysopt sonnection permit-ipsec

```

You can also define dynamic crypto maps:

```

crypto dynamic-map TestDyn 10 match address ACLTest
crypto dynamic-map TestDyn 10 set transform-set TestSet
crypto dynamic-map TestDyn 10 set security-association lifetime
                                                seconds 3600
crypto dynamic-map TestDyn 10 set security-association lifetime
                                                kilobytes 400000
# (optional) define that dynamic crypto map extends the standard one

```

```
crypto map TestMap 20 ipsec-isakmp dynamic TestDyn
```

1.3 Configuring SSH Sentinel

In the SSH Sentinel end, do the following.

1. Create the appropriate pre-shared key. The actual key should naturally be the same as defined in Cisco PIX router.
2. Add a virtual private network connection rule with the following information:
 - Security gateway: The external IP address of the router
 - Remote network: The IP address and netmask of the internal net (10.2.1.0, 255.255.255.0)
 - Authentication key: The pre-shared key you created in the previous step.
 - Proposal template: Legacy proposal. This is a precautionary measure. The normal proposals by Sentinel are potentially too long to be handled by the Cisco PIX router. A legacy proposal is a short form of the proposal. See the SSH Sentinel documentation for details.