VPN Connection to Cisco IOS 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 IOS router acting as a security gateway.

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

Chapter 1

VPN Connection to Cisco IOS 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 IOS router acting as a security gateway.

1.1 Environment

The network environment is illustrated in Figure 1.1 (The network environment) showing the major components. Also, the relevant exemplary IP addresses of various devices are shown. The Cisco IOS 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 IOS security gateway in order to access the private network.

The Cisco IOS version tested is 12.2. Even if the configuration most likely is applicable to other versions, too, it is not guaranteed. Check the Cisco Website for more instructions.

The SSH Sentinel version used in the sample configuration is Sentinel 1.4.

A pre-shared key is used as the authentication method in the configuration. Since both SSH Sentinel and Cisco IOS are capable of using virtual IP addresses, the example also explains how to assign the Sentinel host a virtual IP address.

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

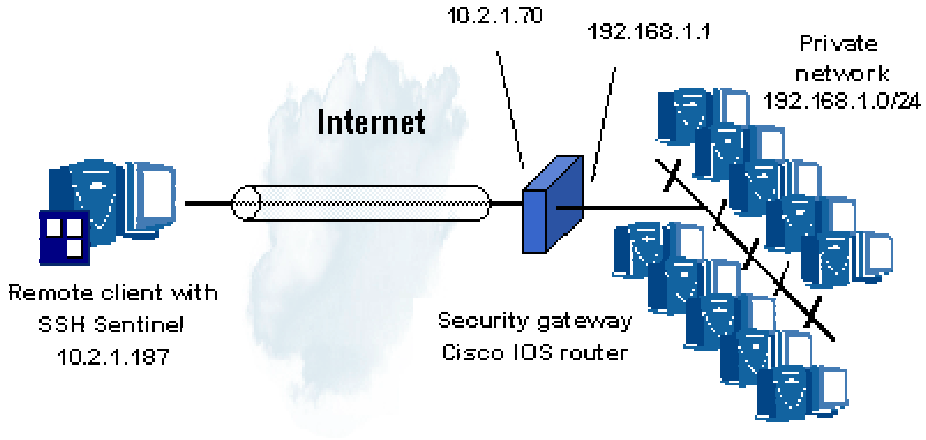

Figure 1.1: The network environment

1.2 Configuring Cisco IOS

This is an actual clip from the output of `running-cfg` on a Cisco IOS router, together with a few comments.

```
# In the following
# md5 specifies the hash function,
# it is declared that a pre-shared key is used for authentication,
# group 2 specifies the Diffie-Hellman group and
# the IKE lifetime is set to 14400 s = 240 min, which is the default
# in SSH Sentinel.

crypto isakmp policy 15
 hash md5
 authentication pre-share
 group 2
 lifetime 14400


# The following defines the pre-shared key for authentication
# when communicating with the remote host 10.2.1.187. The actual key
# is the string 'PreSharedSecret'

crypto isakmp key PreSharedSecret address 10.2.1.187


# This tells which address pool to use to assign the remote peer a
# virtual IP address.
# A pool named PoolIntra is defined, and addresses from 10.2.4.2 to
```

```
# 10.2.4.5 can be assigned to the remote peer.

crypto isakmp client configuration address-pool local PoolIntra
ip local pool PoolIntra 10.2.4.2 10.2.4.5


# This defines a transform set called IosTrans which is used later.

crypto ipsec transform-set IosTrans esp-des esp-md5-hmac


# Crypto maps are used to specify what transforms to use and
# which traffic to encrypt.
# In this case, the traffic to encrypt is not explicitly specified.
# This means that everything will be encrypted.
# The security association lifetime is set to 400000 kB, which is
# the default in SSH Sentinel. The IosTrans transform set defined
# previously is applied.

crypto dynamic-map IosDyn 2
 set security-association lifetime kilobytes 400000
 set transform-set IosTrans


# Defining the crypto map continues. The topmost line here enables
# assigning virtual IP addresses.

crypto map IosMap client configuration address initiate
crypto map IosMap 1 ipsec-isakmp dynamic IosDyn discover


# The interface Ethernet 0 is in this case connected to the Internet.
# See the figure of the network environment for reference.
# The crypto map called IosMap defined previously is applied.
# In other words, traffic from / to outside of the intranet has
# to be encrypted and authenticated.

interface Ethernet0
 ip address 10.2.1.70 255.255.255.0
 no ip directed-broadcast
 no cdp enable
 crypto map IosMap

# The interface Ethernet 1 is in this case connected to the private
# network. See the figure of the network environment for reference.
```



```
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
 no cdp enable
```

1.3 Configuring SSH Sentinel

In the SSH Sentinel end, do the following.

1. Create the appropriate pre-shared key. The actual key must naturally be the same as defined in Cisco.
2. Add a virtual private network connection rule with the following information:
   - Security gateway: The external IP address of the router (in this example, 10.2.1.70)
   - Remote network: The IP address and netmask of the internal net (192.168.1.0, 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 IOS router. A legacy proposal is a short form of the proposal. See the SSH Sentinel documentation for details.
   - Select the check box **Acquire virtual IP address**.

1.4 Configuration without Virtual IP

To configure a virtual IP connection similar to the previous example but not using virtual IP addresses, you have to leave out a few settings from your configurations. On the Cisco side, delete the lines referring to the virtual IP, namely the following in the model setup:

```
# This tells which address pool to use to assign the remote peer a
# virtual address.
# A pool named PoolIntra is defined, and addresses from 10.2.4.2 to
# 10.2.4.5 can be assigned to the remote peer.
# If virtual IP is not used, leave these two lines out.

crypto isakmp client configuration address-pool local PoolIntra
ip local pool PoolIntra 192.168.1.5 192.168.1.10
```

and

```
# Defining the crypto map continues. The topmost line here enables
# assigning virtual IP addresses, leave it out if virtual IP not used.

crypto map IosMap client configuration address initiate
```

In SSH Sentinel, on the connection rule properties, unselect the option **Acquire virtual IP address**.

