



VPN Connection to Cisco VPN 3000 Concentrator

28 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 VPN 3000 Concentrator.

© 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 VPN 3000 Concentrator | 5 |
| 1.1 | Environment | 5 |
| 1.2 | Configuring Cisco VPN 3000 Concentrator | 6 |
| 1.3 | Configuring SSH Sentinel | 10 |
| 1.3.1 | Import the Certificate | 10 |
| 1.3.2 | Create the VPN Rule | 10 |
| 1.4 | Troubleshooting | 11 |

Chapter 1

VPN Connection to Cisco VPN 3000 Concentrator

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 VPN 3000 Concentrator.

1.1 Environment

The network environment is illustrated in Figure 1.1 (The network environment) showing the major components and example IP addresses. The Cisco VPN 3000 Concentrator protects the private network. SSH Sentinel runs on the remote host that contacts the VPN Concentrator in order to access the private network.

The tested hardware model is Cisco VPN 3005 Concentrator with Cisco VPN 3000 Concentrator 3.5.2 software. The SSH Sentinel version used in the sample configuration is SSH Sentinel 1.4.

Certificates are used for authentication. Username and password (extended authentication) are checked against the internal database of the VPN Concentrator. Another possibility would be to use a RADIUS server, for example.

Since both SSH Sentinel and Cisco VPN 3000 Concentrator are capable of using virtual IP addresses, the example also explains how to assign a virtual IP address to the SSH Sentinel host. This example configuration uses L2TP for assigning the virtual IP address. For information on configuring L2TP, refer to http://www.cisco.com/warp/public/471/vpn3k_l2tp.html.

For further information on configuring Cisco VPN 3000 Concentrators, refer to the Cisco VPN 3000 Concentrator manuals available on Cisco's Web site (<http://www.cisco.com/warp/public/707/index.shtml#vpn3000>).

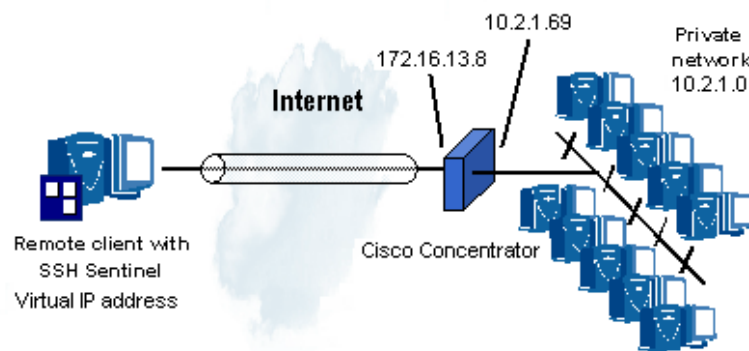


Figure 1.1: The network environment

1.2 Configuring Cisco VPN 3000 Concentrator

1. Connect to the VPN Concentrator console port and verify that correct IP addresses are assigned to its private and public interfaces, and that a default gateway is assigned.

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/getting/gs2inst.htm#xtocid19 for more information.

2. Point a browser to the inside interface of the VPN Concentrator and login as instructed at http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/config/cfgintro.htm.

3. Select **Configuration -> System -> Tunneling Protocols -> IPSec -> IKE Proposals -> Add** to add an Internet Key Exchange (IKE) proposal named Cert+Xauth as shown in Figure 1.2 (Cert+Xauth IKE proposal).

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

| | | |
|---------------------------------|--|--|
| Proposal Name | <input type="text" value="Cert+Xauth"/> | Specify the name of this IKE Proposal. |
| Authentication Mode | <input type="text" value="RSA Digital Certificate (XAUTH)"/> | Select the authentication mode to use. |
| Authentication Algorithm | <input type="text" value="MD5/HMAC-128"/> | Select the packet authentication algorithm to use. |
| Encryption Algorithm | <input type="text" value="3DES-168"/> | Select the encryption algorithm to use. |
| Diffie-Hellman Group | <input type="text" value="Group 2 (1024-bits)"/> | Select the Diffie Hellman Group to use. |
| Lifetime Measurement | <input type="text" value="Time"/> | Select the lifetime measurement of the IKE keys. |
| Data Lifetime | <input type="text" value="10000"/> | Specify the data lifetime in kilobytes (KB). |
| Time Lifetime | <input type="text" value="86400"/> | Specify the time lifetime in seconds. |

Figure 1.2: Cert+Xauth IKE proposal

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/config/tunnel.htm#xtocid2523955 for more information.

4. Activate the IKE proposal.

5. Select **Configuration -> Policy Management -> Traffic Management -> Security Associations -> Add** to add a SA as shown in Figure 1.3 (Security Association).

Modify a configured Security Association.

| | | |
|--------------------|---|---|
| SA Name | <input type="text" value="ESP-3DES-MD5"/> | Specify the name of this Security Association (SA). |
| Inheritance | <input type="text" value="From Rule"/> | Select the granularity of this SA. |

IPSec Parameters

| | | |
|---------------------------------|--|--|
| Authentication Algorithm | <input type="text" value="ESP/MD5/HMAC-128"/> | Select the packet authentication algorithm to use. |
| Encryption Algorithm | <input type="text" value="3DES-168"/> | Select the ESP encryption algorithm to use. |
| Encapsulation Mode | <input type="text" value="Transport"/> | Select the Encapsulation Mode for this SA. |
| Perfect Forward Secrecy | <input type="text" value="Group 2 (1024-bits)"/> | Select the use of Perfect Forward Secrecy. |
| Lifetime Measurement | <input type="text" value="Time"/> | Select the lifetime measurement of the IPSec keys. |
| Data Lifetime | <input type="text" value="10000"/> | Specify the data lifetime in kilobytes (KB). |
| Time Lifetime | <input type="text" value="28800"/> | Specify the time lifetime in seconds. |

IKE Parameters

| | | |
|---------------------------------|--|---|
| IKE Peer | <input type="text" value="0.0.0.0"/> | Specify the IKE Peer for a LAN-to-LAN IPSec connection. |
| Negotiation Mode | <input type="text" value="Main"/> | Select the IKE Negotiation mode to use. |
| Digital Certificate | <input type="text" value="Cisco3005"/> | Select the Digital Certificate to use. |
| Certificate Transmission | <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only | Choose how to send the digital certificate to the IKE peer. |
| IKE Proposal | <input type="text" value="Cert+Xauth"/> | Select the IKE Proposal to use as IKE initiator. |

Figure 1.3: Security Association

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/config/polmgt.htm#xtocid105944 for more information.

6. To assign an address pool for Virtual IP addresses, select **Configuration -> System -> Address Management -> Pools -> Add**. In this example, the Range Start is 10.2.1.131 and Range End 10.2.1.150.

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/config/address.htm#xtocid156678 for more information.

7. Tell the VPN Concentrator to use the address pool by selecting **Configuration -> System -> Address Management -> Assignment** and selecting the **Use Address Pools** check box.
8. For authentication using digital certificates, there must be at least one identity certificate (and its root certificate) installed on the VPN Concentrator. Select **Administration -> Certificate Management** to manage certificates (see Figure 1.4 (Certificate management)).

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/re13_5_1/admin/certman.htm#xtocid1 for more information.

9. Modify a user group by selecting **Configuration -> User Management -> Base Group -> Modify**. Figures 1.5 (Base group, general settings) and 1.6 (Base group, IPSec settings) show the settings for the group.

Administration | Certificate Management Wednesday, 11 September 2002 13:01:59
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities (current: 1, maximum: 6)

| Subject | Issuer | Expiration | SCEP Issuer | Actions |
|-----------------|-----------------|------------|-------------|-------------------------------|
| KuopioCA at SSH | KuopioCA at SSH | 05/07/2004 | Yes | [View Configure Delete] |

Identity Certificates (current: 1, maximum: 2)

| Subject | Issuer | Expiration | Actions |
|------------------|-----------------|------------|---------------------------|
| Cisco3005 at SSH | KuopioCA at SSH | 05/07/2004 | [View Renew Delete] |

SSL Certificate [Generate] *Note: The public key in the SSL certificate is also used for the SSH host key.*

| Subject | Issuer | Expiration | Actions |
|-------------------------------|-------------------------------|------------|---------------------------|
| 10.1.1.100 at Altiga Networks | 10.1.1.100 at Altiga Networks | 09/05/2003 | [View Renew Delete] |

Enrollment Status [Remove All: Errored | Timed-Out | Rejected | Cancelled | In-Progress] (current: 0 available: 2)

| Subject | Issuer | Date | Use | Reason | Method | Status | Actions |
|------------------------|--------|------|-----|--------|--------|--------|---------|
| No Enrollment Requests | | | | | | | |

Figure 1.4: Certificate management

- On the **General** page, select the **L2TP over IPSec** check box and give the **Primary DNS** and **Primary WINS** addresses. The addresses are delivered to the VPN client.
- On the **IPSec** page, select the **Internal** Authentication method, which means that username and password are checked against the internal database of the VPN Concentrator.

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/config/usermgt.htm#xtocid14822 for more information.

10. Add a user by selecting **Configuration -> User Management -> Users > Add**.

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/config/usermgt.htm#xtocid1482202 for more information.

- On the **Identity** page, define the username and password, and select the base group.
- On the **General** page, make the settings as shown in Figure 1.7 (Users, general settings).
- On the **IPSec** page, select the IPSec SA configured in step 5 (in this example, **ESP-3DES-MD5**) as the IPSec SA assigned to this user, and select both **Inherit?** check boxes.

11. Save your configuration.

See http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_5/getting/gs3mgr.htm#xtocid17 for more information.

| General IPSec Mode Config Client FW HW Client PPTP/L2TP | | |
|---|---|--|
| General Parameters | | |
| Attribute | Value | Description |
| Access Hours | -No Restrictions- | Select the access hours for this group. |
| Simultaneous Logins | 3 | Enter the number of simultaneous logins for users in this group. |
| Minimum Password Length | 8 | Enter the minimum password length for users in this group. |
| Allow Alphabetic-Only Passwords | <input checked="" type="checkbox"/> | Enter whether to allow users with alphabetic-only passwords to be added to this group. |
| Idle Timeout | 30 | (minutes) Enter the idle timeout for this group. |
| Maximum Connect time | 0 | (minutes) Enter the maximum connect time for this group. |
| Filter | -None- | Select the filter assigned to this group. |
| Primary DNS | 10.2.1.1 | Enter the IP address of the primary DNS server for this group. |
| Secondary DNS | | Enter the IP address of the secondary DNS server. |
| Primary WINS | 10.2.1.1 | Enter the IP address of the primary WINS server for this group. |
| Secondary WINS | | Enter the IP address of the secondary WINS server. |
| Tunneling Protocols | <input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input type="checkbox"/> IPSec <input checked="" type="checkbox"/> L2TP over IPSec | Select the tunneling protocols this group can connect with. |
| Strip Realm | <input type="checkbox"/> | Check to remove the realm qualifier of the user name during authentication. |

Figure 1.5: Base group, general settings

| General IPSec Mode Config Client FW HW Client PPTP/L2TP | | |
|---|--------------------------|---|
| IPSec Parameters | | |
| Attribute | Value | Description |
| IPSec SA | ESP-3DES-MD5 | Select the IPSec Security Association assigned to this group. |
| IKE Peer Identity Validation | Do not check | Select whether or not to validate the identity of the peer using the peer's certificate. |
| IKE Keepalives | <input type="checkbox"/> | Check to enable the use of IKE keepalives for members of this group. |
| Tunnel Type | Remote Access | Select the type of tunnel for this group. Update the Remote Access parameters below as needed. |
| Remote Access Parameters | | |
| Group Lock | <input type="checkbox"/> | Lock the users into this group. |
| Authentication | Internal | Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication . |
| IPComp | None | Select the method of IP Compression for members of this group. |
| Default Preshared Key | HirmuSalainen | Enter the preshared key to be used with clients that do not support groups. |
| Reauthentication on Rekey | <input type="checkbox"/> | Check to reauthenticate the user on an IKE (Phase-1) rekey. |
| Mode Configuration | <input type="checkbox"/> | Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the the Altiga/Cisco client are being used by members of this group. |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

Figure 1.6: Base group, IPSec settings

| General Parameters | | | |
|----------------------|---|-------------------------------------|--|
| Attribute | Value | Inherit? | Description |
| Access Hours | -No Restrictions- | <input checked="" type="checkbox"/> | Select the access hours assigned to this user. |
| Simultaneous Logins | 3 | <input checked="" type="checkbox"/> | Enter the number of simultaneous logins for this user. |
| Idle Timeout | 30 | <input checked="" type="checkbox"/> | (minutes) Enter the idle timeout for this user. |
| Maximum Connect Time | 0 | <input checked="" type="checkbox"/> | (minutes) Enter the maximum connect time for this user. |
| Filter | -None- | <input checked="" type="checkbox"/> | Enter the filter assigned to this user. |
| Tunneling Protocols | <input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP over IPsec | <input checked="" type="checkbox"/> | Select the tunneling protocols this user can connect with. |

Apply Cancel

Figure 1.7: Users, general settings

1.3 Configuring SSH Sentinel

In the SSH Sentinel end, you need to do two things: import the certificate 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 VPN Concentrator. For basic information on how to manage certificates and connection rules, see the appropriate sections in the SSH Sentinel User Manual.

1.3.1 Import the Certificate

On the **Key Management** page of the Policy Editor, import the certificate needed for authentication. For detailed instructions, see the SSH Sentinel User Manual.

1.3.2 Create the VPN Rule

On the **Security Policy** page of the Policy Editor, select **VPN Connections** and click **Add**. Specify the following values (see Figure 1.8 (The general properties of the VPN rule)):

- Security gateway: The external IP address of the router (in this example, 172.16.13.8, but should be a public IP)
- Remote network: The IP address and netmask of the internal net (in this example, 10.2.1.0, 255.255.255.0)
- Authentication key: The certificate you just imported.

- Proposal template: Legacy proposal. This is a precautionary measure. The normal proposals by SSH Sentinel are potentially too long to be handled by the VPN Concentrator. 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**, click **Settings...**, and select **Layer Two Tunneling Protocol (L2TP)** as the protocol for assigning the virtual IP address.
- Select the check box **Extended authentication**, click **Settings...**, and select **Submit login information automatically**, and give the Login and Password as configured on the VPN Concentrator.

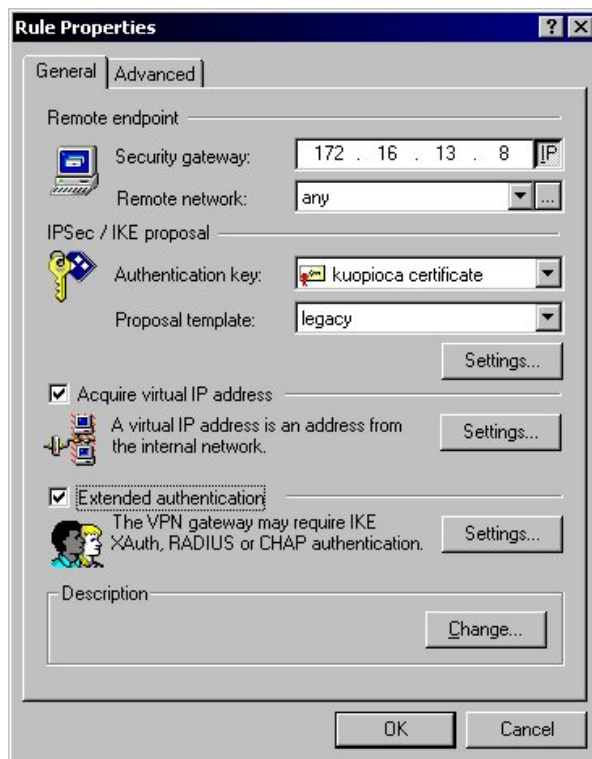


Figure 1.8: The general properties of the VPN rule

1.4 Troubleshooting

To check the status of the current VPN connections to the gateway and to view the VPN log, point the browser to the inside interface of the VPN Concentrator, login, and select **Monitoring -> Live Event Log**.

See <http://www.cisco.com/warp/public/471/vpn3k-conn.html#collect> for more information.

In SSH Sentinel, use the Diagnostics to test the connection. The audit logs and IKE logs are also available for troubleshooting. Refer to the SSH Sentinel User Manual for more information.