



# VPN Connection to Nokia CryptoCluster 500 VPN Gateway

11 December 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 Nokia CryptoCluster 500 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](mailto:ipsec-sales@ssh.com) (sales), [sentinel-support@ssh.com](mailto: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

<b>1</b>	<b>VPN Connection to Nokia CryptoCluster 500 VPN Gateway</b>	<b>5</b>
1.1	Introduction . . . . .	5
1.1.1	Further Information . . . . .	5
1.1.2	Platform Requirements . . . . .	5
1.2	Configuring Nokia CryptoCluster 500 . . . . .	6
1.2.1	Prerequisites . . . . .	6
1.2.2	Enabling Client Access in CryptoCluster . . . . .	6
1.3	Configuring SSH Sentinel . . . . .	9
1.3.1	Prerequisites . . . . .	9
1.3.2	Creating the VPN Rule . . . . .	9
1.4	Troubleshooting . . . . .	11



## Chapter 1

# VPN Connection to Nokia CryptoCluster 500 VPN Gateway

### 1.1 Introduction

This document contains all the required information for setting up a Nokia CryptoCluster 500 (CC500) VPN gateway to accept connections from SSH Sentinel VPN clients. Certificates granted by an external certification authority are used for authentication.

**Note:** For documentation on how to configure other features of CC500, please refer to the Nokia CryptoCluster 500 (CC500) VPN Gateway documentation.

#### 1.1.1 Further Information

- SSH Sentinel User Manual
- SSH Sentinel support: <http://www.ipsec.com>.

#### 1.1.2 Platform Requirements

The interoperability between SSH Sentinel and Nokia CryptoCluster 500 has been tested using the following components:

- SSH Sentinel VPN client v1.4
- Nokia CryptoCluster 500 (CC500) VPN gateway, kernel version 4.0(102)
- Nokia VPN Policy Manager software version 4.0(164).

## 1.2 Configuring Nokia CryptoCluster 500

### 1.2.1 Prerequisites

It is assumed that the initial gateway installation has been performed and that an external certification authority (CA) has been created.

To create a new external CA, open **VPN Global Properties**, select **Policy Configuration -> Certification Authorities** on the left pane, right-click it, and select **New** from the opening menu. Next, select **Import External** and import the external CA certificate into the system.

You can configure the CRL and SCEP settings in the **Settings** page. A request for a gateway certificate can be created under **Gateway Properties -> Certificates -> Device Certificates**.

**Note:** The client certificate used by SSH Sentinel needs to contain an e-mail address in the SubjectAltName field. Otherwise the CryptoCluster gateway will not accept the connection.

### 1.2.2 Enabling Client Access in CryptoCluster

To enable client access, open the **Gateway Properties** window and select **Client Access -> IPSec Clients -> Client Policy** on the left pane.

On the **IKE & IPSec** page, make the following settings (see Figure 1.1 (CryptoCluster Client Policy settings)):

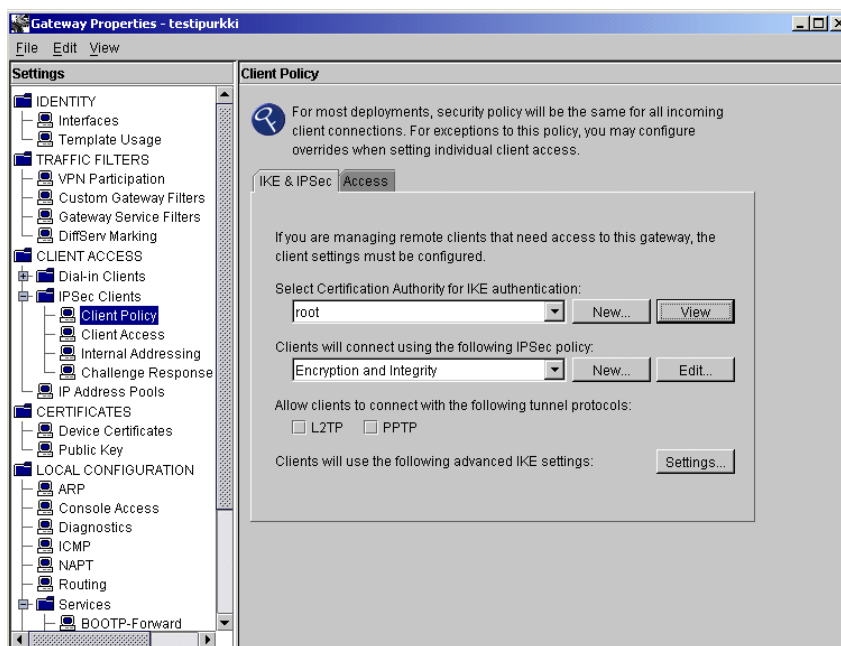


Figure 1.1: CryptoCluster Client Policy settings

1. Select the certification authority for IKE authentication (in this example, `root`).
2. Select **Encryption and Integrity** as the IPsec policy.
3. Click **Edit** to configure the IPsec policy and make the settings shown in Figure 1.2 (CryptoCluster Encryption and Integrity settings):

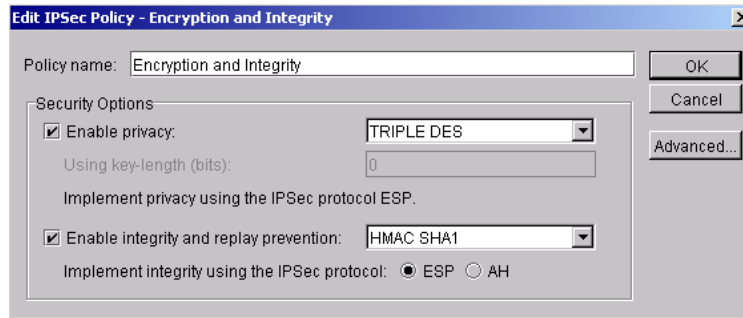


Figure 1.2: CryptoCluster Encryption and Integrity settings

4. Click **Advanced...** and make the settings shown in Figure 1.3 (CryptoCluster Advanced IPsec settings):

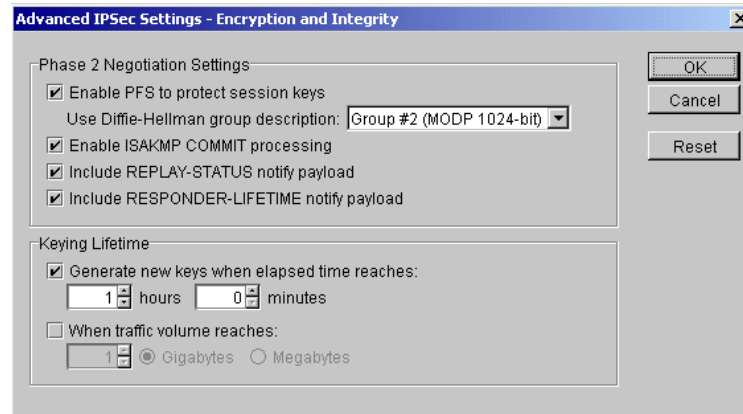


Figure 1.3: CryptoCluster Advanced IPsec settings

5. In the **Client Policy** view, click **Settings...** to configure the **Client IKE Policy**.
6. Select **Edit** to modify an existing IKE policy, or **Add** to create a new one.  
Make the settings shown in Figure 1.4 (CryptoCluster IKE Policy settings) and click **OK** twice to close the dialogs.
7. Click the **Access** tab in the **Client Policy** view and select the access policy that suits your needs.  
This is likely to be **The gateway's protected host groups**. Please note that the host group must match the remote network you define later in SSH Sentinel settings.
8. On the left pane of the of the **Gateway Properties** window, select **Client Access**.

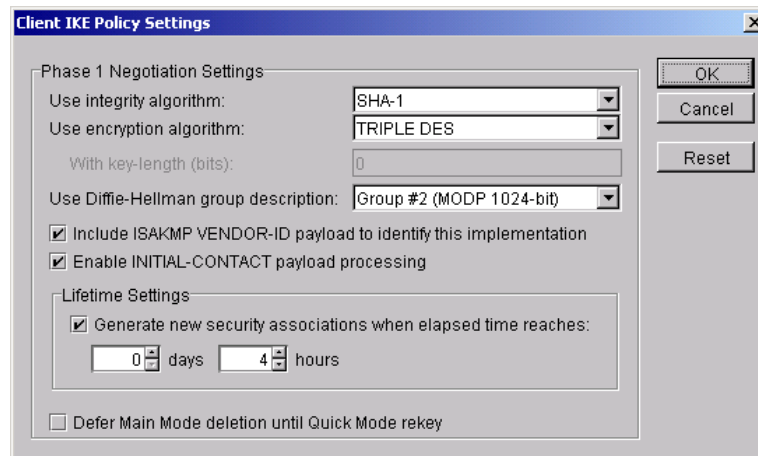


Figure 1.4: CryptoCluster IKE Policy settings

9. Enable **Allow clients to connect using certificate based authentication**, and add a new Certificate Clients entry as shown in Figure 1.5 (CryptoCluster Client Access settings):

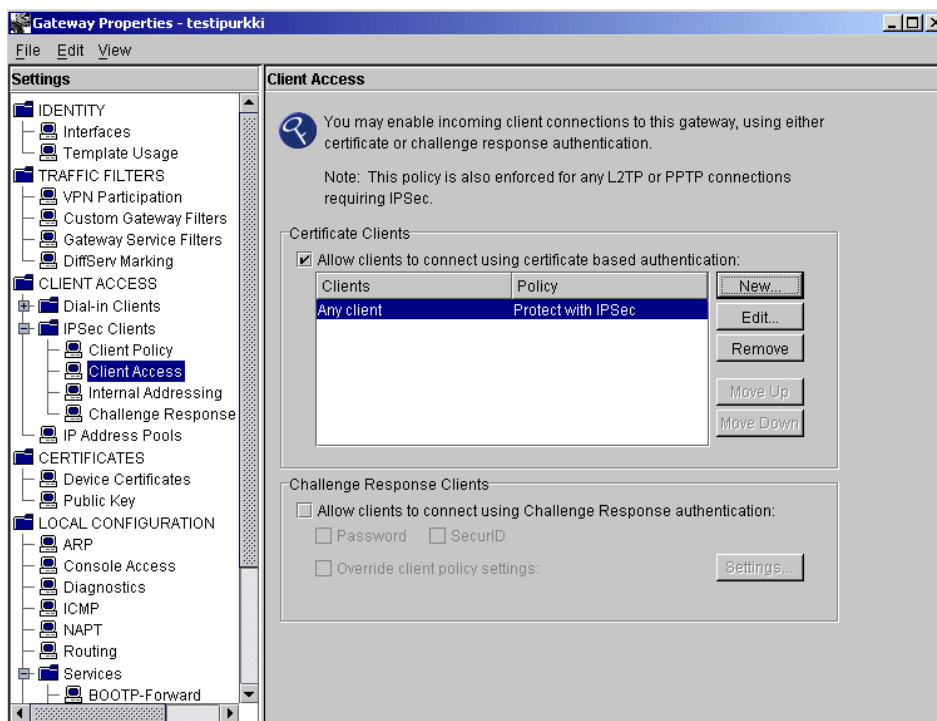


Figure 1.5: CryptoCluster Client Access settings

10. Take the new settings into use by selecting **Actions -> Apply Changes** in the **Policy Manager** main menu.

## 1.3 Configuring SSH Sentinel

### 1.3.1 Prerequisites

It is assumed that a client certificate is already present in SSH Sentinel and that it contains an e-mail address in the `SubjectAltName` field. In addition, you need to add the CA certificate under **Trusted Certificates** -> **Certification Authorities** on the **Key Management** page. For detailed instructions, see the SSH Sentinel User Manual.

The CA certificate properties should be as shown in Figure 1.6 (Certificate properties of the CA certificate) since CRLs are not used in this example configuration:



Figure 1.6: Certificate properties of the CA certificate

### 1.3.2 Creating the VPN Rule

1. 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 (see Figure 1.7 (The general properties of the VPN connection)):

- Security gateway: *the IP address of the gateway*
- Remote network: a network that matches the host group that is protected by the CryptoCluster gateway. For example, if the network behind the gateway is 192.168.1.0/255.255.255.0, create

this network entry in the **Network Editor** (click the ... button to open the editor), and select it as the remote network here.

- Authentication key: select the certificate you wish to use for authentication.
- Proposal template: legacy.

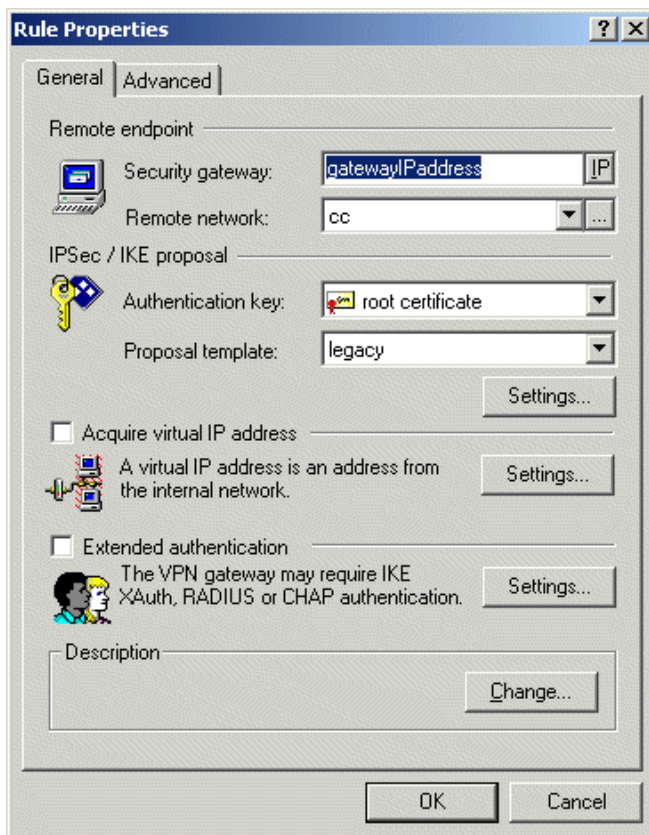


Figure 1.7: The general properties of the VPN connection

2. On the **Rule properties** dialog box, under **IPSec/IKE proposal**, click **Settings** to specify the following:

- IKE proposal
  - Encryption algorithm: 3DES
  - Integrity function: SHA-1
  - IKE mode: main mode
  - IKE group: MODP 1024 (group 2)
- IPSec proposal
  - Encryption algorithm: 3DES
  - Integrity function: HMAC-SHA-1
  - IPSec mode: tunnel
  - PFS group: MODP 1024 (group 2).

3. On the **Advanced** page, the default values for **Security Association Lifetimes** should be OK.  
In addition, select the options **Audit this rule**, **Discover path maximum transfer unit (PMTU)**, and **Deny split tunneling**.
4. Click **OK** and **Apply** to save the settings.
5. Select the CryptoCluster VPN rule and click **Diagnostics** to probe the connection.
6. Open the VPN tunnel via the SSH Sentinel tray icon.
7. Ping the private interface of the router and verify that traffic goes through the VPN tunnel.

## 1.4 Troubleshooting

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