



VPN Connection to Nortel Networks Contivity 600 VPN Gateway

30 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 Nortel Networks Contivity 600 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 Nortel Networks Contivity 600 VPN Gateway	5
1.1	Environment	5
1.2	Configuring Nortel Networks Contivity 600 VPN Gateway	6
1.3	Configuring SSH Sentinel	10
1.3.1	Import the Certificate	10
1.3.2	Create the VPN Rule	10

Chapter 1

VPN Connection to Nortel Networks Contivity 600 VPN Gateway

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 Nortel Networks Contivity 600 VPN gateway.

1.1 Environment

The environment is illustrated in Figure 1.1 (The network environment) showing the major components and example IP addresses. The Nortel Networks Contivity 600 VPN gateway protects the private network. SSH Sentinel runs on the remote host that contacts the gateway in order to access the private network.

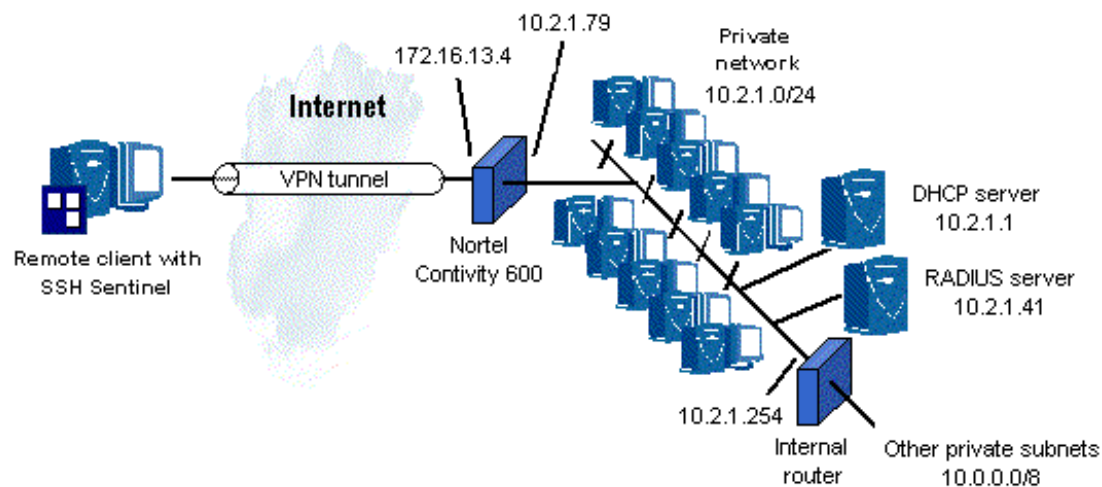


Figure 1.1: The network environment

The tested Nortel Networks Contivity 600 VPN gateway version is v04_00.89. 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 an external RADIUS accounting database.

Since both SSH Sentinel and Nortel Networks Contivity 600 VPN gateway 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 further information on configuring the gateway, refer to the Contivity manuals on the Nortel Networks Web site (<http://www.nortelnetworks.com/products/01/contivity/600/>).

1.2 Configuring Nortel Networks Contivity 600 VPN Gateway

1. Connect to the Web-based Nortel Networks management system.
2. Make the following **SYSTEM** settings:
 - **Identity:**
 - Management IP Address: 10.2.1.79
 - Primary DNS Server Address 10.2.1.1.
 - **LAN Interfaces** as shown in Figure 1.2 (The LAN interface settings).
 - **Certificate Configuration** as shown in Figure 1.3 (The Certificate Configuration settings).
 - **Forwarding:**
 - Proxy ARP for Branch Office Tunnels.

Interface	Description	State	Type	Actions
LAN		Enabled	Private	<input type="button" value="Configure"/> <input type="button" value="Statistics"/>

IP Address	Subnet Mask	Interface Filter	Actions
10.2.1.78	255.255.255.0	deny all (Contivity Interface Filter not in use)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Interface	Description	State	Type	Actions
Slot 1 Interface 1		Enabled	Public	<input type="button" value="Configure"/> <input type="button" value="Statistics"/>

IP Address	Subnet Mask	Interface Filter	Actions
172.16.13.4	255.255.255.0	deny all (Contivity Interface Filter not in use)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure 1.2: The LAN Interfaces settings

Certificate Signature Requirements

Key Usage Extension Required

Installed Tunnel and Transport Certificates

Enable 'Allow All' Feature*

Trusted	Type	Allow All		Subject DN	Validity	Actions	
		Enabled	Default Group				
<input checked="" type="checkbox"/>	CA	<input checked="" type="checkbox"/>	/Base	CN=KuopioCA, OU=SSH Kuopio, O=SSH, C=FI	05/08/2002 - 05/07/2004	Delete	Details
<input checked="" type="checkbox"/>	Server	N/A	N/A	CN=nortel, ST=Eastern Finland, L=Kuopio, OU=Kuopio QA, O=SSH, C=FI	06/20/2002 - 05/07/2004	Delete	Details

Import Tunnel or Transport Certificate

Generate Certificate Request

Certificate Management Protocol (CMP) PKCS#10 Certificate Request

* Authenticates any user or machine presenting a valid certificate from the associated CA.

Figure 1.3: The Certificate Configuration settings

3. Make the following **SERVICES** settings (**Note** that Contivity 600 supports 3DES, but all Contivity models do not):

- **Available:**

Tunnel Type: IPsec, PPTP and L2TP & L2P: both Public and Private
 Management Protocol: HTTP, SNMP, CRL Retrieval, and CMP: Private

- **IPSec:**

Authentication: User Name and Password/Pre-Shared Key and RSA Digital Signature
 RADIUS Authentication: User Name and Password
 Encryption: ESP- Triple DES with MD5 Integrity, ESP- 56 bit DES with MD5 Integrity, and ESP - 40 bit DES with MD5 Integrity
 IKE Encryption and Diffie-Hellman Group: Triple DES with Group 2 (1024-bit prime)
 NAT Traversal: Enabled, UPD port 2746
 Authentication Order: as shown in Figure 1.4 (The Authentication Order settings)

Authentication Order

Order	Server	Type	Associated Group	Action
1	LDAP	Internal		
2	RADIUS	CHAP, PAP	/Base	Delete

Add LDAP Authentication Server

Figure 1.4: The Authentication Order settings

Leave other settings blank.

- **L2TP:**

Authentication: CHAP and PAP

Authentication Order: as shown in Figure 1.4 (The Authentication Order settings)

- **Syslog :**

Line 1: Enabled, Host IP Address 10.2.1.41, Message Level Normal, Facility KERN, UDP Port 514.

Leave the **RADIUS** settings blank because the internal RADIUS service is not used. We use extended authentication with an external RADIUS server instead (declared in the **SERVERS -> RADIUS Auth** settings).

4. Make the **ROUTING -> Static Routes** settings as shown in Figure 1.5 (The Routing settings)

Static Routes

Enabled

OK Cancel

Default Routes

Type	Gateway Address	Interface	Admin State	Cost	Action
Public	172.16.13.254	Slot 1 Interface 1	Enabled	1	Edit Delete

Add Public Route Add Private Route

Static Routes through Physical Interfaces

IP Address	Subnet Mask	Gateway Address	Interface	Admin State	Cost	Action
10.0.0.0	255.0.0.0	10.2.1.254	LAN	Enabled	10	Edit Delete

Add

Show Branch Office Routes

Figure 1.5: The Routing settings

5. Make the following **PROFILES -> Groups** settings:

Select the **/Base** group and click **Edit**. Make sure that all the settings are as configured above.

Note that no local users are declared under **Users**. External RADIUS service is used instead.

6. Make the following **SERVERS** settings:

- **RADIUS Auth** as shown in Figure 1.6 (The RADIUS Authentication settings)

Enable the Primary RADIUS server, give IP address 10.2.1.41 for the server, select Private interface (10.2.1.79), and port 1812.

- **RADIUS Acct** (Accounting):

Enable Internal RADIUS Accounting

Enable External RADIUS Accounting Server at address 10.2.1.41, port 1813.

Enable Access to RADIUS Authentication

Remove Suffix from User ID (e.g. jsmith@nortelnetworks.com)
 Delimiter Value=

RADIUS Users Obtain Default Settings from the Group

Server-Supported Authentication Options

Enabled	Type	Description
<input type="checkbox"/>	CHALLENGE	Challenge/Response Token Cards
<input type="checkbox"/>	RESPONSE	Response Only Token Cards
<input type="checkbox"/>	MS-CHAP	MSCHAP - Microsoft encrypted CHAP. <input type="checkbox"/> RFC-2548 (Microsoft Vendor-specific RADIUS Attributes) compliant
<input checked="" type="checkbox"/>	CHAP	CHAP - Challenge Handshake Authentication Protocol.
<input checked="" type="checkbox"/>	PAP	PAP - Password Authentication Protocol.

Figure 1.6: The RADIUS Authentication settings

- **User IP Addr:** External DHCP server is used for assigning the IP addresses for SSH Sentinel clients. Make the settings as shown in Figure 1.7 (The Remote User IP Address Pool settings).

DHCP

Any DHCP Server
 Specified DHCP Server

DHCP Server	IP Address	Status
Primary	<input type="text" value="10.2.1.1"/>	Configured
Secondary	<input type="text" value="0.0.0.0"/> *Optional	Not Configured
Tertiary	<input type="text" value="0.0.0.0"/> *Optional	Not Configured

DHCP Cache Size

Immediate Address Release

DHCP Blackout Interval* (seconds) *Amount of time before an address is available for issue.

Override Blackout Interval when no addresses are available

Figure 1.7: The Remote User IP Address Pool settings

- Leave the **LDAP**, **LDAP Auth** (Authentication), and **DHCP Relay** settings blank.

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 Nortel Networks Contivity gateway.

1.3.1 Import the Certificate

Enroll a certificate from a CA that is trusted by your Nortel Networks gateway. The CA may be the same that you used to get host certificate for the Contivity gateway itself.

Import the certificate on the **Key Management** page of the Policy Editor. 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 connection):

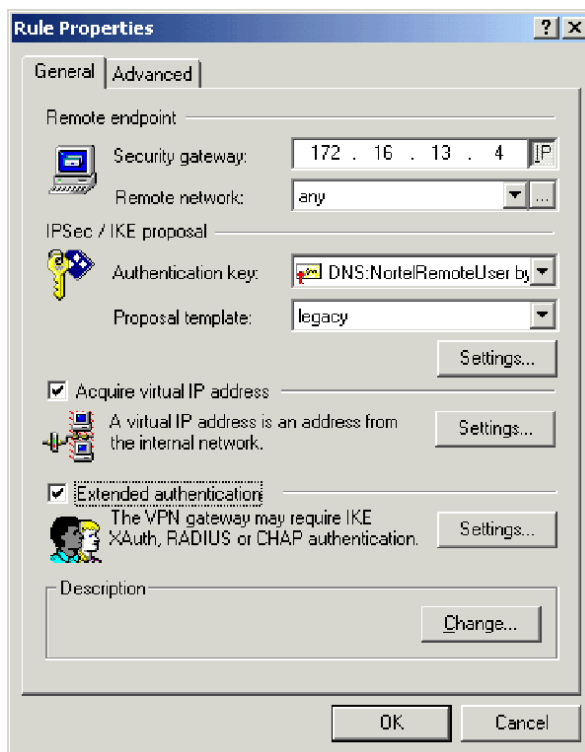


Figure 1.8: The general properties of the VPN connection

- Security gateway: The external IP address of the gateway (in this example, 172.16.13.4)
- 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 gateway. 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 **Specify DNS and WINS servers** and give the IP addresses of the name servers located in your target private network (in this example, 10.2.1.1 for both).
- Select the check box **Extended Authentication**, click **Settings...**, and select **Submit login information automatically**, and give the Login and Password as configured on the external RADIUS database server that the Nortel Networks Contivity gateway is configured to relay on.
- Select **OK** to save the VPN rule and **Apply** to deploy the new settings.
- Select the Contivity VPN rule and click **Diagnostics** to probe the connection. If everything was configured properly, you will see the Diagnostics dialog box shown in Figure 1.9 (The diagnostics).

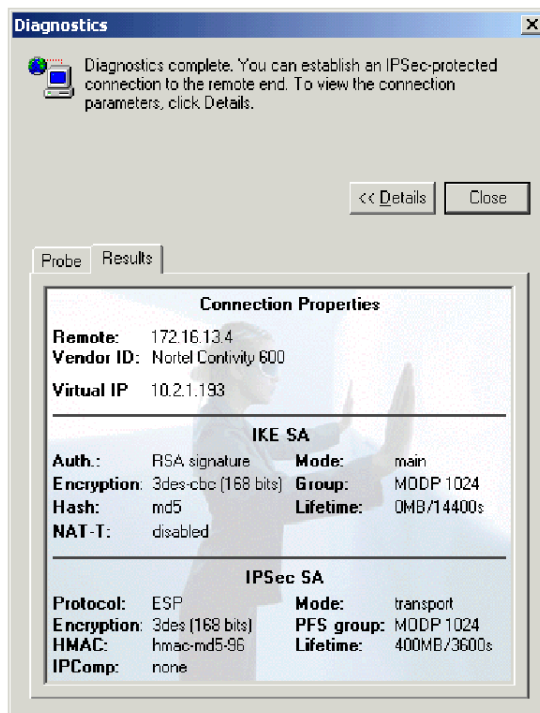


Figure 1.9: The diagnostics

In this example, the private DHCP server used gave SSH Sentinel virtual IP address 10.2.1.193. All the traffic from the SSH Sentinel client seems to be coming from that source address.