



Best Practices:

How to configure Nokia Mobile VPN Client
with Preshared Key authentication (case Cisco)

November 2005



1. Introduction

This best practices document describes how to configure Nokia Mobile VPN Client, when Nokia Mobile VPN client uses *Preshared Key authentication* method in the *Cisco VPN 3000 Series Concentrator v4.7* environment.

The Preshared Key authentication method is less secure than other traditional authentication methods and therefore it should only be used in test (non-production) environments.

This document describes also how to create and install VPN policies to the mobile devices manually i.e. without the policy server (Nokia Security Service Manager).

2. Installing the VPN policy

This chapter provides information and a procedure to create VPN policies for the Nokia Mobile VPN Client and convert the VPN policies into packages that users can install on mobile devices.

The VPN policy needs to be packaged into a *Symbian Installation System* (SIS) file that can be installed in the same ways as any Symbian software.

To create a VPN policy manually the following files are needed:

- `Makesis.exe`
 - Windows command line utility to create SIS files
- Policy information file (*.pin)
 - Contains additional information about the VPN policy e.g. the name of the VPN policy
- Policy file (*.pol)
 - Contains actual VPN policy settings e.g. IKE and IPSec settings
- Package file (*.pkg)
 - Contains settings for the *.sis file and lists installable files and their locations in the device

2.1 Creating the VPN policy information file (PIN)

Create the policy information file **VPN-policy-preshared-cisco.pin** with the following content:

```
[POLICYNAME]
VPN Policy
[POLICYDESCRIPTION]
VPN-policy-preshared-cisco.pol for Nokia Mobile VPN Client v3.0.
[POLICYVERSION]
1.1
[ISSUERNAME]
Do not edit
[CONTACTINFO]
Do not edit
```

You may use other text under the [POLICYNAME] and [POLICYDESCRIPTION] sections.

2.2 Creating the VPN policy file (POL)

Create the policy (text) file **VPN-policy-preshared-cisco.pol** with the following content:

```
SECURITY_FILE_VERSION: 3
[INFO]
VPN-policy-preshared-cisco.pol for Nokia Mobile VPN Client v3.0.
[POLICY]
sa ipsec_1 = {
  esp
  encrypt_alg 12
  max_encrypt_bits 256
  auth_alg 3
  identity_remote 0.0.0.0/0
  pfs
  src_specific
  hard_lifetime_bytes 0
  hard_lifetime_addtime 3600
  hard_lifetime_usetime 3600
  soft_lifetime_bytes 0
  soft_lifetime_addtime 3600
  soft_lifetime_usetime 3600
}

remote 0.0.0.0 0.0.0.0 = { ipsec_1(123.45.67.89) }

inbound = { }
outbound = { }

[IKE]
ADDR: 123.45.67.89 255.255.255.255
MODE: Aggressive
SEND_NOTIFICATION: TRUE
ID_TYPE: 11
FODN: PreSharedGroup
GROUP_DESCRIPTION_II: MODP_1536
USE_COMMIT: FALSE
IPSEC_EXPIRE: FALSE
SEND_CERT: FALSE
INITIAL_CONTACT: FALSE
RESPONDER_LIFETIME: TRUE
REPLAY_STATUS: TRUE
USE_INTERNAL_ADDR: FALSE
USE_NAT_PROBE: FALSE
ESP_UDP_PORT: 0
NAT_KEEPALIVE: 60
USE_XAUTH: TRUE
USE_MODE_CFG: TRUE
REKEYING_THRESHOLD: 90
PROPOSALS: 1
ENC_ALG: AES256-CBC
AUTH_METHOD: PRE-SHARED
HASH_ALG: SHA1
GROUP_DESCRIPTION: MODP_1536
GROUP_TYPE: DEFAULT
LIFETIME_KBYTES: 0
LIFETIME_SECONDS: 28800
PRF: NONE
PRESHARED_KEYS:
FORMAT: STRING_FORMAT
KEY: 8 password
```

These settings define the actual VPN policy and they must match exactly with the corresponding settings in the Cisco gateway. The chapter 4 describes how to configure the Cisco gateway to match with the settings of this example VPN policy file. If you use other values, the corresponding values must be used in Cisco.

Special notes:

- For *encrypt_alg* the available values are **2** (DES), **3** (3DES) and **12** (AES).
- For *auth_alg* the available values are **2** (MD5) and **3**(SHA1).
- *USE_XAUTH* and *USE_MODE_CFG* must be set to **TRUE**
- *USE_NAT_PROBE* must be set to **FALSE** and *ESP_UDP_PORT* must be set to **0**
- *MODE* must be set to **Aggressive**
- Create a user group in Cisco with the same name as the value of *FQDN* e.g *PreSharedGroup*
- Define the password for this group (PreSharedGroup) in Cisco to match the value of *KEY*

2.3 Creating the VPN package file (PKG)

Create the package file **VPN-policy-preshared-cisco.pkg** with the following content:

```
;
; A VPN POLICY PACKAGE
;

; LANGUAGES
; - None (English only by default)

; INSTALLATION HEADER
; - Only one component name is needed to support English only
; - UID is the UID of the VPN Policy Installer application
; #{"VPN Policy"},{0x1000597E},1,0,0,TYPE = SISCONFIG

; LIST OF FILES

; Policy file
"VPN-policy-preshared-Cisco.pol"- "C:\System\Data\Security\Install\VPN-policy-preshared-Cisco.pol"

; Policy-information file
; - NOTE: The policy-information file MUST be the last file in this
; list!
; - FM (FILEMIME) passes the file to the respective MIME handler
; (in this case, the VPN Policy Installer
; application).
"VPN-policy-preshared-Cisco.pin"- "C:\System\Data\Security\Install\VPN-policy-preshared-Cisco.pin",
FM, "application/x-ipsec-policy-info"

; REQUIRED FILES
; - The VPN Policy Installer application
(0x1000597E), 1, 0, 0, {"VPN Policy Installer"}
```

Note that this file expects that the name of the policy information file is **VPN-policy-preshared-cisco.pin** and the name of the policy file is **VPN-policy-preshared-cisco.pol**.

2.4 Creating the Symbian Installation file (SIS)

Store all the four (4) files in the same directory in the Windows PC and run the following command:

makesis VPN-policy-preshared-cisco.pkg

As a result of this command the SIS file **VPN-policy-preshared-cisco.sis** is generated.

2.5 Installing the VPN policy

Deliver the file **VPN-policy-preshared-cisco.sis** to mobile device running Nokia VPN Client.

The installation starts when you open the SIS file in the mobile phone.
You may also use PC Suite for the VPN policy installation.

3. Configuring the Mobile VPN Client

In this document, Nokia 9500 (or 9300) phone is used as a configuration example.

To use the VPN policy with the Nokia VPN Client you will need to create a *VPN Access Point* and associate it with the VPN policy. Therefore select *Tools* → *Control Panel* → *Connections* → *VPN Access Points* → *New* to create a VPN access point. Enter a descriptive name for the VPN access point e.g. *VPN*. Associate the VPN access point with the VPN policy and the real Internet Access Point (IAP). For the *Network* setting use "VPN" (should differ from the IAP's corresponding Network setting).

To use VPN connection you should associate the VPN access point with the applications in 9500.
Below an example on how to configure email to use VPN connection.

Select *Messaging* → *Menu* → *Tools* → *Account settings* → your mailbox → *Edit*.
Under *General* → *Internet Access* select your VPN access point.

4. Configuring Cisco 3000

Use *VPN 3000 Concentrator Series Manager* to configure Cisco VPN 3000 Concentrator.
The *VPN 3000 Concentrator Series Manager* is started by taking HTTP connection with the WWW browser to the IP address of the Internal (Private) Interface of Cisco 3000.
Log On as admin.
After completing the listed steps below remember to save the configurations before exiting the tool.

4.1 Configuring Internal Addressing

The use of Internal Addressing is optional but highly recommended due to its benefits e.g. easier routing from corporate Intranet back to VPN clients and possibility to utilize corporate DNS service.

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *System* → *Address Management* → *Pools* → *Add* to add an Internal address pool.
Select *Configuration* → *System* → *Address Management* → *Assignment* to define how the VPN Clients obtain the IP address. Check the *Use Address Pools* box and click *Apply*.
Then select *Configuration* → *User Management* → *Base Group* → *General* tab to define corporate (internal) DNS servers (primary and secondary). Click *Apply*.

4.2 Configuring NAT-Traversal (NAT-T)

Cisco 3000 supports IETF NAT-T implementation that uses UDP port 4500.

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *Tunneling and Security* → *IPSec* → *NAT Transparency* and check the *IPSec over NAT-T* box. Click *Apply*.

4.3 Configuring Remote Client Access using Preshared Key Authentication

4.3.1 Configuring IKE (Phase 1) settings

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *Tunneling and Security* → *IPSec* → *IKE Proposals* → *Add* to add a new IKE proposal. See Picture 1.

Enter a descriptive name for the IKE Proposal e.g. *IKE-PSK*.
Select *Preshared Keys (XAUTH)* in the *Authentication Mode* list
For the other IKE settings, select

- *SHA/HMAC-160* in the *Authentication Algorithm* list
- *AES-256* in the *Encryption Algorithm* list
- *Group 5 (1536-bits)* in the *Diffie-Hellman Group* list
- *28800* for the *Time Lifetime*

Click *Add*.

Move the proposal to the *Active Proposals* list and move it to the top of the list.

Configuration | Tunneling and Security | IPSec | IKE Proposals | Add

Configure and add a new IKE Proposal.

Proposal Name	<input type="text" value="IKE-PSK"/>	Specify the name of this IKE Proposal.
Authentication Mode	<input type="text" value="Preshared Keys (XAUTH)"/>	Select the authentication mode to use.
Authentication Algorithm	<input type="text" value="SHA/HMAC-160"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="AES-256"/>	Select the encryption algorithm to use.
Diffie-Hellman Group	<input type="text" value="Group 5 (1536-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="28800"/>	Specify the time lifetime in seconds.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

Picture 1: IKE Proposal for Remote Access using Preshared Keys authentication

4.3.2 Configuring IPSec (Phase 2) settings

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *Policy Management* → *Traffic Management* → *SAs* → *Add* to add a new IPSec SA. See Picture 2.

Enter a descriptive name for the IPSec SA e.g. *PSK-SA*.

Under the section *IPSec Parameters*, select

- *ESP/SHA/HMAC-160* in the *Authentication Algorithm* list
- *AES-256* in the *Encryption Algorithm* list
- *Group 5 (1536-bits)* in the *Perfect Forward Secrecy* list
- *3600* for the *Time Lifetime*

Under the section *IKE Parameters*, select

- *Aggressive* in the *Negotiation Mode* list
- *None (Use Preshared Keys)* in the *Digital Certificate* list
- *IKE-PSK* in the *IKE Proposal* list

Click *Add*.

Configuration | Policy Management | Traffic Management | Security Associations | Add

Configure and add a new Security Association.

<p>SA Name <input type="text" value="PSK-SA"/></p> <p>Inheritance <input type="text" value="From Rule"/></p>	<p>Specify the name of this Security Association (SA).</p> <p>Select the granularity of this SA.</p>
--	--

IPSec Parameters

<p>Authentication Algorithm <input type="text" value="ESP/SHA/HMAC-160"/></p> <p>Encryption Algorithm <input type="text" value="AES-256"/></p> <p>Encapsulation Mode <input type="text" value="Tunnel"/></p> <p>Perfect Forward Secrecy <input type="text" value="Group 5 (1536-bits)"/></p> <p>Lifetime Measurement <input type="text" value="Time"/></p> <p>Data Lifetime <input type="text" value="10000"/></p> <p>Time Lifetime <input type="text" value="3600"/></p>	<p>Select the packet authentication algorithm to use.</p> <p>Select the ESP packet encryption algorithm to use.</p> <p>Select the Encapsulation Mode for this SA.</p> <p>Select the use of Perfect Forward Secrecy.</p> <p>Select the lifetime measurement of the IPSec keys.</p> <p>Specify the data lifetime in kilobytes (KB).</p> <p>Specify the time lifetime in seconds.</p>
--	--

IKE Parameters

<p>IKE Peer <input type="text" value="0.0.0.0"/></p> <p>Negotiation Mode <input type="text" value="Aggressive"/></p> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p>IKE Proposal <input type="text" value="IKE-PSK"/></p>	<p>Specify the IKE Peer for a LAN-to-LAN connection.</p> <p>Select the IKE Negotiation mode to use.</p> <p>Select the Digital Certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Select the IKE Proposal to use as IKE initiator.</p>
---	--

Picture 2: IPSec SA settings for Remote Access using Preshared Keys authentication

4.3.3 Creating a user group for users using Preshared Keys Authentication

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *User Management* → *Groups* → *Add Group* to add a new user group.

Under the *Identity* tab,

- enter a descriptive name for the user group e.g. *PreSharedGroup*
- enter password in the *Password* text box
- select *Internal* in the *Type* list

Under the *IPSec* tab,

- select *PSK-SA* in the *IPSec SA* list
- check the *IKE Keepalives* box to enable Dead-Peer-Detection feature
- select *Remote Access* in the *Tunnel Type* list
- select one of the following alternatives in the *Authentication* list
 - *Internal* (if using Cisco's internal database for authentication)
 - *RADIUS* (if using external RADIUS server for authentication)
 - *Kerberos/Active Directory* (if using external AD server for authentication)
- Select *None* in the *IPComp* list
- Check the *Mode Configuration* box

Click *Add*.

4.3.4 Configuring external authentication servers

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *System* → *Servers* → *Authentication*, and press *Add* to add to an external authentication server.

To use RADIUS server

- select *RADIUS* in the *Server Type* list
- enter IP address or hostname in the *Authentication Server* text box
- enter port number in the *Server Port* (1645 or 1812) text box
- enter the server secret in the *Server Secret* text box

To use Active Directory server

- select *Kerberos/Active Directory* in the *Server Type* list
- enter IP address or hostname in the *Authentication Server* text box
- enter port number in the *Server Port* (0 or 88) text box
- enter domain e.g. LDAP.NOKIA.COM in the *Realm* text box (note uppercase!)

4.3.5 Creating a local user for Preshared Keys Authentication

At *VPN 3000 Concentrator Series Manager* select *Configuration* → *User Management* → *Users* → *Add* to add a new user. This is only needed if you use Cisco's internal database for user authentication.

Under the *Identity* tab,

- enter the name and password for the user
- enter the group to which the user belongs e.g. *PreSharedGroup*

About Nokia

Nokia is the world leader in mobile communications, driving the growth and sustainability of the broader mobility industry. Nokia is dedicated to enhancing people's lives and productivity by providing easy-to-use and secure products like mobile phones, and solutions for imaging, games, media, mobile network operators and businesses. Nokia is a broadly held company with listings on five major exchanges.

For more information, please visit <http://www.nokia.com/forbusiness>.

Americas

Nokia

313 Fairchild Drive, Mountain View, CA 94043

Tel: 1 877 997 9199

Email: mobile.business.americas@nokia.com

Europe, Middle East and Africa

Nokia

Nokia House, Summit Avenue

Southwood, Hampshire, GU14 0NG, UK

Tel UK: +44 161 601 8908

Tel France: +33 170 708 166

Email: mobile.business.emea@nokia.com

Asia Pacific

Nokia

438B Alexandra Road

#07-00 Alexandra Technopark, Singapore 119968

Tel: +65 6588 3364

Email: mobile.business.apac@nokia.com

www.nokia.com

NOKIA

CONNECTING PEOPLE

Copyright© 2004 Nokia. All rights reserved. Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Other trademarks mentioned are the property of their respective owners. Nokia operates a policy of continuous development. Therefore we reserve the right to make changes and improvements to any of the products described in this document without prior notice. Under no circumstances shall Nokia be responsible for any loss of data or income or any direct, special, incidental, consequential or indirect damages howsoever caused. .