Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of

Patient Summary and Electronic Prescription

VPN problems tracking and resolution

APPENDIX D

D 3.B.2

WORK PACKAGE	**WP3.B**
DOCUMENT NAME	VPN problems tracking and resolution
SHORT NAME	VPN ISSUES
DOCUMENT VERSION	**1.0**
DATE	**28/12/2013**

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	**VPN problems tracking and resolution**
Document Short name:	**VPN ISSUES**
Distribution level	**PU**
Status	**Draft**
Author(s): Organization:	OpenNCP Community **OpenNCP Community**

Dissemination level: PU = Public, PP = Restricted to other programme participants, RE = Restricted to a group specified by the consortium, CO = Confidential, only for members of the consortium.

ABSTRACT
"VPN problems tracking and resolution: representsa basic reproduction from the online documentation created by the OpenNCP Community while tracking, diagnosing and solving VPN related issues that affected the epSOS pilots.

Change History					
Version	Date	Status Changes	From	Details	Review
V1.0	28/12/13	Draft	L.Mano	Reproduced from the OpenNCP Knowledge Repository	Licinio Mano Marcello Melgara

5

TABLE OF CONTENTS

1 Introduction

This information is presented with more operational details in the online documentation, available at:

https://openncp.atlassian.net/wiki/display/ODC/VPN+problems+tracking+and+resolution

Even though, this document aims to document the major findings emerged from the work accomplished and make them available for further understanding.

2 How to use this documentation

1. Check the existent "**Common problem and solutions"** section, for a possible answer;

2. Present you problem as a comment at the bottom of the page, providing as much as feedback as possible (**Description**, **Error messages, and other useful information**);

3. Fill your system setup configuration parameters (OpenSwan and OS version);

```
You can check the OpenSwan version with the following command:
ipsec verify
```

4. Fill the **status matrix**, painting the background with the corresponding color **GREEN** (symbol), **RED** (symbol), accordingly (if you do not fill, this task will be done by the page moderator);

```
You can check the connectivity with a certain country with the following command:
ipsec barf 2>&1 | grep -i ESTAB | grep -i '"COUNTRY CODE"'
```

5. For easy access you can put a comment link in the status symbol, just go to the comment, right click the **Date** at the bottom of the comment and copy the link, then paste the link with the symbol as the name. (See Portuguese example)

6. Wait for possible feedback, provided by the task-force;

3 Common problems and solutions

3.1 Potential problems and potential solutions

1. Problem #1 - Firewall Rules

Problem Name	Firewall Rules
Description	It is not enough just to open the Tomcat SSL port 8443 for connections with other NCPs. There are some additional ports that must be opened for IPsec to work. Here is the specification.
Solutions	TCP/8443* HTTPS *See note below UDP/500 Internet Security Association and Key Management Protocol (ISAKMP) UDP/4500 IPSec NAT Traversal (SAE-URN) IP forwarding must be enabled at the firewall for the following IP protocols and UDP ports: IP Protocol ID 50: For both inbound and outbound filters. Should be set to allow Encapsulating Security Protocol (ESP) traffic to be forwarded. IP Protocol ID 51: For both inbound and outbound filters. Should be set to allow Authentication Header (AH) traffic to be forwarded. UDP Port 500: For both inbound and outbound filters. Should be set to allow ISAKMP traffic to be forwarded. * Note that if you are using an external firewall, and the VPN tunnel terminates at your NCP, there is no need to open the port 8443 at the external firewall. If it is open, it might seem that the VPN connection works, while in fact communication is going directly and not through the VPN. In the NCP's own firewall (e.g. iptables) the port 8443 must of course be open.

2. Problem #2 - Why and How to setup a VPN as an epSOS PN/NCP?

Problem Name	Why and How to setup a VPN as an epSOS PN/NCP?
Description	A good practice manual, for epSOS PN to follow, that describes how a VPN should be setup.
Solutions	IHE - epSOS PPT - VPN setup **http://gazelle.ihe.net/content/epsos-ppt-vpn-setup-0** ***http://gazelle.ihe.net/content/epsos-ppt-vpn-setup*** (deprecated)

3. Problem #3 - Verify if firewall ports are open

Problem Name	Verify if firewall ports are open
Description	Commands to verify if the appropriate firewall ports are open
Solutions	**UDP PORTS** nmap -sU -p U:50,51,500,4500 -PN <IP_ADDRESS> **TCP PORTS** nmap -p T:50,51,500,4500 -PN <IP_ADDRESS>

4. Problem #4 - OpenSwan development is stalled

Problem Name	OpenSwan development is stalled. OpenSwan fails to support current VPN standards.
Description	Some Linux distributions stop supporting OpenSwan. For example: **https://www.suse.com/releasenotes/x86_64/SUSE-SLES/11-SP3/#fate-312973** *L3 support for Openswan is scheduled to expire. This decision is driven by the fact that Openswan development stalled substantially and there are no tangible signs that this will change in the future.* In contrast to this the strongSwan project is vivid and able to deliver a complete implementation of current standards. Compared to Openswan all relevant features are available by the package strongSwan plus strongSwan is the only complete Open Source implementation of the RFC 5996 IKEv2 standard whereas OpenSwan only implements a small mandatory subset. For now and the expected future only strongSwan qualifies to be an enterprise-ready solution for encrypted TCP/IP connectivity.

Solutions	Switch to strongSwan and IKEv2. FI tried this with HR. This does not work because strongSwan does not support NAT traversal in transport mode by default. It must be compiled with a switch, see **https://lists.strongswan.org/pipermail/users/2010-October/005355.html** The problem still remains. The switch to strongSwan might help in case there are no NATs involved. The connection FI-ES seemed to go up (but documents exchange was not verified) when Finland switched from openSwan to strongSwan.

5. Problem #5 - Connection can be started only from one part (one direction connectivity)

Problem Name	Connection can be started only from one part (one direction connectivity)
Description	Luxembourg can initiate the connection with many PN's but none can initiate the connection with LU
Solutions	Possible solution should be Luxembourg to use public IP address without NAT. Solved after re-installing certificates in ipsec using tslsync and removing before it all certificates. There is a possibility of corrupted exported certificates. So, I should recommend to do the following: 6. Check firewall status using the provided in this wiki page commands (nmap) 7. Check with ipsec verify that ipsec starts correctly 8. Check that certificates have been imported correctly to ipsec directory or database. Possible rerun of tslsync with prior deletion of certificates

Other ideas:

Are the problems connected with different Linux kernel versions? The problems in Finland started about at the same time when a new SLES distribution was installed, with a switch in the Linux kernel version from 2.x to 3.x? Ipsec uses some kernel modules, and this might affect the situation. Writing info on linux kernel versions in different countries might help investigating this.

3.2 What was tried and what does not seem to help

70

Are the problems connected with certificates?

Finland and Spain tried using self-signed certificates generated in Finland using Kostas' generation scripts. This did not help solving the problem with FI-ES connection, which currently does not work despite neither part is behind NAT.

75 Estonia and Hungary was able to establish connection using Estonian test certificates and Hungarian PPT certificates. We were unable to connect with Estonian PPT certificates. The Estonian PPT certificates themselves are valid.

Are the problems connected with openSwan versions?

80 Finland tried switching from openSwan 2.6.14 to 2.6.38, this did not have any impact on the number of running connections.