

	Site to Site Virtual Private Networks			
	Programme	<i>NPFIT</i>	DOCUMENT RECORD ID KEY	
	Sub-Prog / Project	<i>Information Governance</i>	<i>NPFIT-FNT-TO-IG-GPG-0002.01</i>	
	Prog. Director	<i>Mark Ferrar</i>		
	Owner	<i>Tim Davis</i>	Version	<i>1.0</i>
	Author	<i>Phil Benn</i>		
	Version Date	<i>22/02/2006</i>	Status	<i>APPROVED</i>

## Site to Site Virtual Private Networks (VPNs): Good Practice Guidelines

**Amendment History:**

Version	Date	Amendment History
0.1	22/08/2005	First draft for comment
1.0	16/02/2006	Approved

**Forecast Changes:**

Anticipated Change	When
Annual Review	March 2007

**Reviewers:**

This document must be reviewed by the following. Indicate any delegation for sign off.

Name	Signature	Title / Responsibility	Date	Version
Malcolm McKeating		IG Security Team Manager		1.0
Tim Davis		Head of Information Governance		1.0

**Approvals:**

This document requires the following approvals:

Name	Signature	Title / Responsibility	Date	Version
Tim Davis		Head of Information Governance		1.0
Mark Ferrar		Director Of Technical Infrastructure		1.0

**Distribution:**

Information Governance website: <http://nww.connectingforhealth.nhs.uk/>

**Document Status:**

This is a controlled document.

This document version is only valid at the time it is retrieved from controlled filestore, after which a new approved version will replace it.

On receipt of a new issue, please destroy all previous issues (unless a specified earlier issue is baselined for use throughout the programme).

**Related Documents:**

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	12

## Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
	Abstract.....	5
1.1	Aims and Objectives .....	5
1.2	Assumed Reader Knowledge .....	5
1.3	Background .....	6
1.4	Disclaimer.....	6
<b>2</b>	<b>Virtual Private Networks: An Overview .....</b>	<b>7</b>
2.1	Secure VPNs .....	7
2.2	Trusted VPNs .....	7
<b>3</b>	<b>Selecting and deploying VPN hardware .....</b>	<b>7</b>
3.1	Site-to-site VPN using a router, concentrator or gateway .....	7
3.2	Site-to-site VPN using a firewall .....	8
<b>4</b>	<b>Configuration of IPSec VPNs.....</b>	<b>8</b>
4.1	Encryption.....	8
4.2	Traffic Authentication .....	9
4.3	Device Authentication using Digital Certificates and Preshared Keys	9
4.4	Site- to-Site VPNs over the Internet.....	10
4.5	Intrusion Detection.....	10
<b>5</b>	<b>Glossary.....</b>	<b>11</b>

# 1 Introduction

## Abstract

This guide addresses the major issues associated with creating and maintaining secure Virtual Private Networks (**VPNs**) using the New NHS Network (**N3**). Detailed technical knowledge of the techniques presented is not required.

The following information covers all environments required to interact with the NHS Care Records Service (**NCRS**). It includes an overview of the subject, information on suitable hardware and configuration details for the most secure solutions that conform with the Connection for Digital Services.

You will find best practice guidance for deploying and using VPNs. This includes:

- The minimum standards for Site to Site VPNs.
- The procedures and mechanisms for the secure control of Site to Site VPNs in an NHS or other healthcare environment

## 1.1 Aims and Objectives

The following information provides a knowledge-based framework that will help maintain best practice values in your own organisation. In using this guide you will be conforming to best practice and therefore avoid some of the consequences of non-compliance.

After completing this guide you should understand:

- Good practice for organisations who wish to deploy, or operate, Site to Site VPNs in a NHS or other healthcare environment.
- The types of VPN available, the different methods of deploying a site to site VPN and how to securely configure a VPN.

## 1.2 Assumed Reader Knowledge

- A general familiarity with firewalls, switches and routers and secure networking practices.

Further information on network security and related matters is available from the NHS Connecting for Health Information Governance website.

## 1.3 Background

N3 is a private Wide Area Network (**WAN**). Connection is therefore strictly limited to authorised endpoints. All organisations wishing to make a new connection to N3 are responsible for ensuring that their connection to the WAN does not compromise the security measures already in place.

- N3 is a private network consisting of thousands of PCs, servers, printers and other items of equipment all acting as the nodes or endpoints on the network. Information is unencrypted when transmitted over the network therefore confidentiality of sensitive information within N3 is not assured. However, all National Applications encrypt data using Transport Layer Security (**TLS**). It is therefore advisable for Existing Systems to take the appropriate measures to ensure that sensitive data is secure before connecting to N3.
- N3 faces numerous threats to security as a result of incompletely protected partner networks or connections to uncontrolled external networks such as the internet. These threats are continually evolving in both strength and frequency: ongoing vigilance against these threats and the maintenance of strict security standards are essential to the continuing success of N3.

## 1.4 Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NHS Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NHS Connecting for Health shall also accept no responsibility for any errors or omissions contained within this document. In particular, NHS Connecting for Health shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

## 2 Virtual Private Networks: An Overview

A VPN offers trusted or secured connectivity over a shared network infrastructure such as N3 or the Internet. VPNs allow traffic to be carried using standard networking protocols while maintaining the integrity of data transported.

### 2.1 Secure VPNs

Secure VPNs use cryptographic tunnelling protocols to provide the confidentiality, integrity and authentication of data to achieve the intended level of privacy. Secure VPN protocols can include Internet Protocol Security (**IPSec**), Secure Socket Layer (**SSL**) and Point-to-Point Tunnelling Protocol (**PPTP**).

### 2.2 Trusted VPNs

Trusted VPNs do not use cryptographic tunnelling protocols and therefore rely on the security of a single service provider's infrastructure to provide the required level of security. Multi-Protocol Label Switching (**MPLS**) is often used to build trusted VPNs; this is a key element of virtual Wide Area Networks as supplied by a number of communications service providers.

Other technologies used to build trusted VPNs are Layer 2 Forwarding (**L2F**) and Layer 2 Tunnelling Protocol (**L2TP**).

## 3 Selecting and deploying VPN hardware

Organisations should ensure that each VPN endpoint has a suitable networking device installed. The device should be one of the following types:

- A router with the appropriate IPSec software
- A firewall with software support for IPSec VPNs
- A VPN concentrator or gateway.

### 3.1 Site-to-site VPN using a router, concentrator or gateway

It is possible to construct a VPN between two points on a network using a dedicated IPSec capable device such as a router, concentrator or gateway. There are two options for deploying this type of device:

- **Inside the network:** A Common Criteria Evaluation Assurance Level 4 (**EAL4**) certified firewall protects each perimeter of the VPN device.

The access controls on the firewall should allow the IPSec encapsulated traffic, including associated key exchange traffic, to pass through - they should also filter all other traffic inbound and outbound.

- **Outside the network:** Achieved via a single direct connection to a dedicated interface on an EAL4 approved firewall. This interface should be separate from both the internal and external interfaces of the firewall and should filter all traffic appropriately. The VPN transit cable connection (or VLAN) should be kept isolated from any other connection. It should not be used for any purpose other than:
  - a) Transporting traffic to the VPN device for encapsulation.
  - b) Transporting traffic from the VPN device following de-encapsulation.

### 3.2 Site-to-site VPN using a firewall

It is possible to construct a VPN between two points on a network using an IPSec capable firewall. The device should be EAL4 certified and configured to perform filtering on all traffic which traverses the system - including any traffic transported across the VPN tunnel. This device might be the primary firewall system for the site, or possibly an additional system used for the sole purpose of VPN connectivity.

Please be aware that if the VPN firewall is located behind another EAL4 certified device, the VPN firewall does not have to be EAL4 certified. This scenario may be applicable to smaller organisations who wish to use site-to-site VPNs while retaining the perimeter firewall services provided by N3.

## 4 Configuration of IPSec VPNs

### 4.1 Encryption

It is recommended that encryption - to a minimum of Advanced Encryption Standard 128 (**AES-128**) - is used to provide sufficient confidentiality for data traversing a site-to-site VPN. However, consideration for Triple Data Encryption Standard (**3DES** or **Triple DES**) encryption – to a minimum standard of 3DES 112 - might be preferable for systems which do not include AES support.

Further information on suitable encryption algorithms is available in the *Approved Cryptographic Algorithms: Good Practice Guidelines* document.



The 3DES block cipher is generally more resource-intensive than the AES block cipher. Systems which do not include hardware cryptographic accelerators should consider the use of AES to achieve higher throughput.

## 4.2 Traffic Authentication

When deploying site-to-site VPNs it is important that you use a form of traffic authentication such as the Authentication Header (**AH**) protocol.

However, it may be preferable to consider an Encapsulating Security Payload Authentication Algorithm (**ESP-AUTH**). Essentially this performs a similar function within the ESP protocol -without the separate requirement to use the AH protocol. Each IP datagram has the ESP-AUTH header and trailer appended to it, allowing the authentication of the original source packet once it reaches the VPN peer endpoint.

It is recommended that the Secure Hash Algorithm (**SHA-1**) with either ESP-AUTH or AH is used to protect the integrity of traffic.

Please note that the Message Digest 5 (**MD5**) hashing algorithm is vulnerable to certain cryptographic attacks and should not be used.

## 4.3 Device Authentication using Digital Certificates and Preshared Keys

The use of certificates to authenticate VPN peers is recommended, as it provides a known framework in which devices can be authenticated. Tunnel or Security Association (**SA**) re-keying times should be based on both time and data, with a re-key after either 8 hours or 500MB of data, whichever occurs first.

Preshared keys could be an alternative solution if the construction and operation of a Public Key Infrastructure (**PKI**) infrastructure is not practicable. Please note:

- Preshared keys should be set to a minimum length of 25 alphanumeric/symbol characters.
- Information Security best practices for password selection need to be applied when selecting preshared keys.

## 4.4 Site- to-Site VPNs over the Internet

When passing private communications across a public infrastructure (such as a site-to-site VPN across the internet) it is important to mitigate the increased risks this attracts by taking increased security precautions:

- Use a Common Criteria EAL4 firewall device to separate the N3 system from the internet and ensure that no traffic is routable between the two entities, directly or indirectly.
- For site-to-site traffic the VPN endpoint device needs accreditation to a minimum of CC EAL3.
- The VPN endpoint device needs accreditation to a minimum of CC EAL4 if it also connects directly to both the internal network and the internet without a separate firewall in place.
- When determining the required traffic filtering rules and policies appropriate to each site it is important to follow Information Security best practices.

## 4.5 Intrusion Detection

At nodes of internet access the deployment of an Intrusion Detection or Prevention System (**IDS/IPS**) may be particularly beneficial. Deployment should include branch sites such as GP surgeries and health centres if they choose to utilise Internet connectivity rather than N3.

To ensure that no element of the secure network architecture has been overlooked a full penetration test performed by a CHECK-approved tester should be undertaken. This needs to include testing of the VPN infrastructure and any directly connected system.

Further information is available within the *Intrusion Detection Systems and Intrusion Protection Systems: Good Practice Guidelines* document.

## 5 Glossary

- 3DES:** See Triple DES (below).
- AES-128:** Advanced Encryption Standard 128. An encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies, that may eventually become the de facto encryption standard for commercial transactions in the private sector.
- AH:** Authentication Header. An IPsec protocol that provides for anti-replay and verifies that the contents of the packet have not been modified in transit. AH is a mathematical code that is embedded and transmitted in the IP packet.
- DES:** Data Encryption Standard. A cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm is a sixteen round block cipher which uses a 64bit block and a 56bit key.
- EAL4:** Evaluation Assurance Level 4. A specification method standardising commonly found requirements. Lists what the system is supposed to do and expresses (using a number from one and seven) the degree of confidence that you can place in the system.
- ESP-AUTH:** Encapsulating Security Payload Authentication Algorithm. An IPsec protocol that provides data confidentiality (encryption), anti-replay, and authentication. ESP encapsulates data in the IP packet and may be applied alone or in combination with AH.
- IDS:** Intrusion Detection System. An Intrusion Detection System monitors any network traffic and logs/notifies any possible malicious activity.
- IPS:** Intrusion Prevention System. Any device which exercises access control to protect computers from exploitation. Intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator.
- IPSec:** Internet Protocol Security. A method of securing IP communications for security that takes place at the network or packet processing layer of network communication.
- ISAKMP:** Internet Security Association and Key Management Protocol. A protocol for establishing Security Associations (**SA**) and cryptographic keys in an internet environment. ISAKMP defines the procedures for: authenticating a communicating peer, creation and management of Security Associations, key

generation techniques and threat mitigation (e.g. denial of service and replay attacks).

- L2F:** Layer 2 Forwarding protocol. An extension of the Point-to-Point Tunnelling Protocol (**PPTP**) used by an Internet service provider (**ISP**) to enable the operation of a virtual private network (**VPN**) over the Internet. L2TP merges the best features of two other tunnelling protocols: PPTP from Microsoft and L2F from Cisco Systems.
- L2TP:** Layer 2 Tunnelling Protocol. A tunnelling protocol used to support virtual private networks (VPNs).
- MD5:** Message Digest 5. A standard algorithm that takes as input a message of arbitrary length and produces as output a 128-bit fingerprint or message digest of the input. Any modifications made to the message in transit can then be detected by recalculating the digest.
- MPLS:** Multiprotocol Label Switching. A standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to.
- N3:** The New NHS Network. A private Wide Area Network consisting of thousands of PCs, servers, printers and other items of equipment. Information is unencrypted when transmitted over the network therefore confidentiality of sensitive information within N3 is not assured.
- NCRS:** NHS Care Records Service. The new terminology for what was previously called ICRS. This is the public facing terminology for the electronically stored health care records for patients. It will be held partially at a national level on the National Data Spine and partly at a local level by the Local Service Providers.
- PKI:** Public Key Infrastructure. Enables users of a basically unsecured public network (such as the internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair, obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
- PPP:** Point to Point Protocol. A data transfer protocol which operates at the Data Link Layer.

- PPTP:** Point to Point Tunnelling Protocol. Allows existing Network Access Server (NAS) functions to be separated using a client-server architecture, where many functions would have been previously serviced by a NAS. PPTP also offers the facility to tunnel a Point to Point Protocol (**PPP**) session over an IP network.
- SA:** Security Association. A relationship between two or more entities that describes how they will utilise security services to communicate securely
- SHA-1:** Secure Hash Algorithm. A message digest algorithm developed by the NSA for use in the Digital Signature standard. SHA is an improved variant of MD4 producing a 160-bit hash. SHA is one of two message digest algorithms available in IPsec. The other is **MD5**.
- SSL:** Secure Sockets Layer. A protocol designed to provide secure communications across the Internet.
- TLS:** Transport Layer Security. A protocol designed to provide secure communications across the Internet designed as a successor to SSL. It uses the same cryptographic methods but supports more cryptographic algorithms.
- Triple DES:** Also referred to as **3DES**. A mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).
- VPN:** Virtual Private Network. A private data network that makes use of the public telecommunication infrastructure; privacy is maintained through the use of a tunnelling protocol and security procedures.
- WAN:** Wide Area Network. A computer network that spans a relatively large geographical area, typically a WAN consists of two or more local-area networks (**LANs**). The largest WAN in existence is the internet.