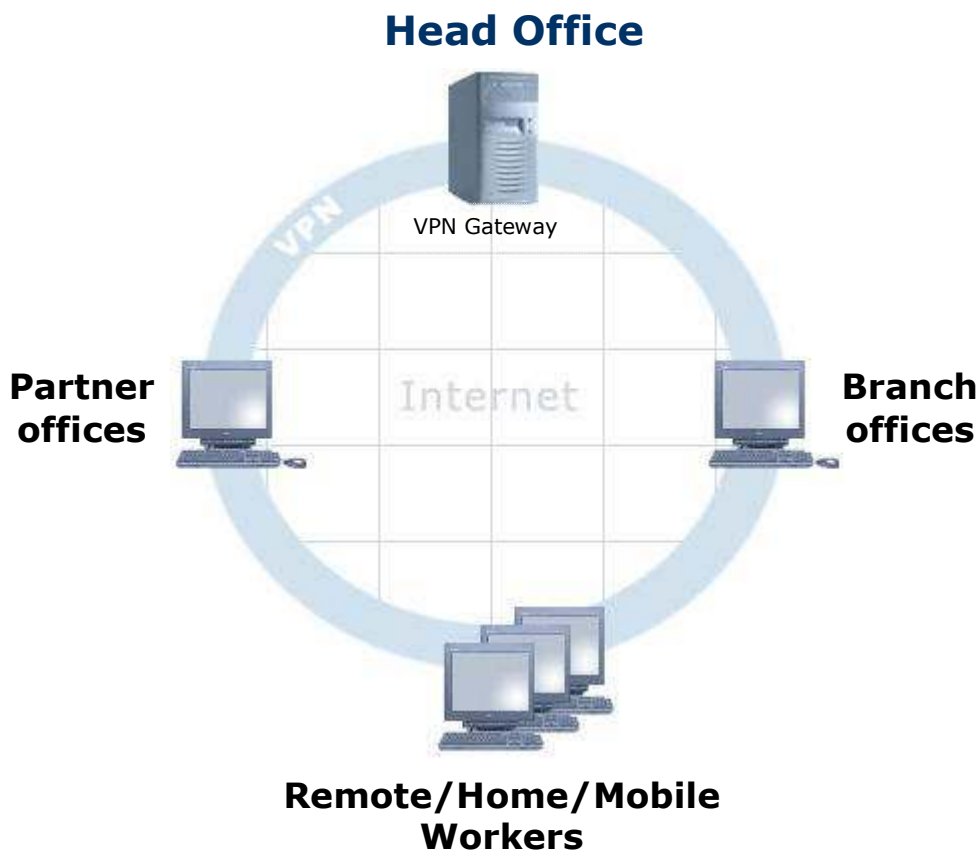


IPSec VPN Guide Users Manual

4.0



Copyright © 2007, F/X Communications. All Rights Reserved. The use and copying of this product is subject to a license agreement. Any other use is strictly prohibited. No part of this publication may be reproduced, transcribed, or translated into any language, in any form by any means without the prior written consent of F/X Communications. Information in this document is subject to change without notice and does not constitute any commitment on the part of F/X Communications.

Contents

1. INTRODUCTION	5
1.1. DOCUMENT SCOPE	5
1.2. READING THIS DOCUMENT.....	5
I. Learning about InJoy IPsec	6
2. IPSEC TECHNOLOGY OVERVIEW	7
2.1. WHAT IS A VIRTUAL PRIVATE NETWORK (VPN)?.....	7
2.2. INTRODUCTION TO IPSEC	8
3. INJOY IPSEC FEATURES	12
3.1. TRAFFIC ENCAPSULATION MODES.....	12
3.2. ENCRYPTION METHODS.....	12
3.3. AUTHENTICATION METHODS	13
3.4. ROAD WARRIORS	14
3.5. KEY MANAGEMENT	15
3.6. IPSEC EXTENSIONS.....	15
II. Getting Started	17
4. STARTING IPSEC	18
4.1. INJOY IPSEC REQUIREMENTS	18
4.2. ENABLING THE IPSEC SOFTWARE COMPONENTS.....	19
4.3. VERIFYING IPSEC SUPPORT	20
5. CONFIGURATION OVERVIEW	21
5.1. WHAT NEEDS CONFIGURATION?	21
5.2. HOW IS IPSEC CONFIGURED?	21
5.3. WHICH IPSEC CONFIGURATION FILES EXIST?	23
5.4. HOW DO I ACTIVATE CONFIGURATION CHANGES?	26
6. USING THE QUICK VPN WIZARD	28
6.1. VPN WIZARD OVERVIEW	28
6.2. STARTING THE VPN WIZARD.....	30
6.3. SETTING UP A VPN SERVER OR CLIENT	31
6.4. CONFIGURING VPN USERS	34
7. USING THE TUNNEL WORKSHOP	35
7.1. CREATING SECURITY ASSOCIATIONS	35
7.2. EDITING EXISTING SECURITY ASSOCIATIONS.....	40
7.3. SAMPLE SECURITY ASSOCIATIONS	41
8. USING INJOY IPSEC	42
8.1. BASIC ARCHITECTURE	42
8.2. MONITORING USERS AND TUNNELS.....	42
8.3. LOGGING AND TRACE FILES.....	44
8.4. FAIL-OVER AND FALL-BACK.....	45
8.5. TRANSFORM ORDER CONTROL.....	45
8.6. PERFECT FORWARD SECRECY (PFS)	46
8.7. SELECTIVELY BYPASSING THE TUNNEL	46
8.8. PATH MTU DISCOVERY.....	46
8.9. HEARTBEATS AND TUNNEL LIVELINESS.....	47
8.10. LIMITATIONS.....	47
III. Setting up a VPN	48

9. IPSEC DEPLOYMENT PLANNING.....	49
9.1. THE IPSEC PLANNING WORKSHOP	49
9.2. IDENTIFYING YOUR IPSEC ENDPOINTS.....	57
9.3. DEFINING YOUR IKE NEGOTIATION POLICIES	58
9.4. DEFINING YOUR ENCRYPTION AND HASHING POLICIES	59
9.5. USING IPSEC EXTENSIONS	60
10. A VPN CASE STUDY	62
10.1. SOFTDEV.COM: VPN PLANNING	62
10.2. HEAD OFFICE VPN SERVER CONFIGURATION	64
10.3. PARTNER COMPANY CONFIGURATION	74
10.4. REMOTE EMPLOYEES CONFIGURATION.....	76
10.5. ESTABLISHING THE TUNNEL.....	78
10.6. MONITORING AND MAINTENANCE	79

IV. Advanced Features Guide 80

11. USING ROAD WARRIOR SUPPORT	81
11.1. INTRODUCTION TO ROAD WARRIORS.....	81
11.2. ROAD WARRIOR LIMITATIONS.....	82
11.3. OPERATIONAL DETAILS	83
11.4. SAMPLE ROAD WARRIOR SCENARIOS	84
12. USING INNER-IP SUPPORT	87
12.1. INTRODUCTION TO INNER-IP	87
12.2. INNER-IP LIMITATIONS.....	88
12.3. OPERATIONAL DETAILS	89
12.4. SAMPLE INNER-IP SCENARIOS	89
13. USING IPSEC BEHIND NAT	91
13.1. INTRODUCTION TO NAT TRAVERSAL.....	91
13.2. NAT-T OPERATION DETAILS	92
13.3. NAT-T LIMITATIONS	93
14. USING IP COMPRESSION	95
14.1. INTRODUCTION TO IP COMPRESSION.....	95
14.2. IP COMPRESSION CONFIGURATION	96
15. USING MANUAL KEYING	98
15.1. INTRODUCTION TO MANUAL KEYING.....	98
15.2. MANUAL KEYING DRAWBACKS	98
15.3. USING MANUAL KEYING	98
16. AUTHENTICATION METHODS	101
16.1. PRE-SHARED KEYS	101
16.2. EXTENDED AUTHENTICATION (XAUTH)	102
16.3. RSA DIGITAL SIGNATURES	105
16.4. GROUP AUTHENTICATION	109
16.5. X.509 CERTIFICATES.....	111

V. Deployment Examples 119

17. MORE SAMPLE SCENARIOS	120
17.1. SIMPLE VPN USING MANUAL KEYING	120
17.2. SIMPLE VPN USING AUTOMATIC KEYING	122
17.3. VPN WITH MULTIPLE SUB-NETWORKS	123
17.4. VPN USING RSA DSS AUTHENTICATION	127
17.5. VPN USING NAT-T AND VPN GATEWAY	130

VI. References	133
18. APPENDIX A – UTILITY PROGRAMS	134
18.1. "IPSEC" (IPSEC MANAGEMENT UTILITY).....	134
18.2. "RSASIGKEY" (RSA SIGNATURE GENERATION)	135
19. APPENDIX B - IPSEC INTEROPERABILITY	136
20. APPENDIX C – PROTOCOL SUPPORT SUMMARY	138
21. APPENDIX D – CONFIGURATION ATTRIBUTES	140
21.1. SECURITY ASSOCIATIONS ("IPSEC.CNF")	140
21.2. IPSEC OPTIONS ("OPTIONS.CNF").....	151

1

Introduction

IPSec is a transparent security layer for TCP/IP that is commonly used to create and operate Virtual Private Networks (VPNs).

The InJoy IPSec implementation is one of the few end-to-end VPN solutions that is both standards-based and available for multiple Operating Systems.

1.1. Document Scope

This document is designed to provide a concise introduction to IPSec and guide you through its configuration.

Before setting up a VPN, you should be familiar with TCP/IP and the InJoy products of choice. TCP/IP networking should be functioning properly between any hosts you plan to include in your VPN.

Because IPSec represents an addition to your operating system's networking layer, rather than an application or tool, the number of possible configurations and uses for IPSec are endless. This document will provide you with enough instruction to address most common needs.

1.2. Reading This Document

This document has been divided into several distinct parts according to the amount of information different types of readers are likely to need:

Part I.	Learning about InJoy IPSec
Part II.	Getting Started Guide
Part III.	Setting up a VPN
Part IV.	Advanced Features Guide
Part V.	Deployment Examples
Part VI.	References

If you are looking to set up a VPN in the fastest possible way, please refer to section 6, "Using the Quick VPN Wizard".

For a more comprehensive real-world example, please refer to section 10, "A VPN Case Study."

[Click here to download full PDF material](#)