
**Information technology — Security
techniques — Network security —**

Part 3:

**Reference networking scenarios —
Threats, design techniques and control
issues**

*Technologies de l'information — Techniques de sécurité — Sécurité de
réseau —*

*Partie 3: Scénarios de réseautage de référence — Menaces,
techniques conceptuelles et questions de contrôle*

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Structure.....	3
6 Overview.....	4
7 Internet access services for employees	6
7.1 Background.....	6
7.2 Security threats	7
7.3 Security design techniques and controls	7
8 Business to business services	9
8.1 Background.....	9
8.2 Security threats	9
8.3 Security design techniques and controls	10
9 Business to customer services	11
9.1 Background.....	11
9.2 Security threats	11
9.3 Security design techniques and controls	12
10 Enhanced collaboration services	13
10.1 Background.....	13
10.2 Security threats	14
10.3 Security design techniques and controls	14
11 Network segmentation	15
11.1 Background.....	15
11.2 Security threats	15
11.3 Security design techniques and controls	15
12 Networking support for home and small business offices	16
12.1 Background.....	16
12.2 Security threats	16
12.3 Security design techniques and controls	17
13 Mobile communication.....	18
13.1 Background.....	18
13.2 Security threats	18
13.3 Security design techniques and controls	19
14 Networking support for travelling users	20
14.1 Background.....	20
14.2 Security threats	20
14.3 Security design techniques and controls	20
15 Outsourced services	21
15.1 Background.....	21
15.2 Security threats	21
15.3 Security design techniques and controls	22
Annex A (informative) An Example Internet Use Policy.....	23
Annex B (informative) Catalogue of Threats	27