ISO/IEC 27033-4:2014-03 (E)

Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Abbreviated terms 2

5 Structure 4

6 Overview 4

7 Security threats 5

8 Security requirements 6

9 Security controls 8
9.1 Overview 8
9.2 Stateless packet filtering 8
9.3 Stateful packet inspection 9
9.4 Application firewall 9
9.5 Content filtering 10
9.6 Intrusion prevention system and intrusion detection system 10
9.7 Security management API 11

10 Design techniques 11
10.1 Security gateway components 11
10.2 Deploying security gateway controls 12

11 Guidelines for product selection 16
11.1 Overview 16
11.2 Selection of a security gateway architecture and appropriate components 17
11.3 Hardware and software platform 17
11.4 Configuration 17
11.5 Security features and settings 18
11.6 Administration capability 19
11.7 Logging capability 19
11.8 Audit capability 20
11.9 Training and education 20
11.10 Implementation types 20
11.11 High availability and operation mode 20
11.12 Other considerations 20

Bibliography 22