ISO/IEC 18028-3:2005-12 (E)

Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 4

5 Security requirements 5

6 Techniques for security gateways 5
6.1 Packet filtering 5
6.2 Stateful packet inspection 6
6.3 Application proxy 6
6.4 Network Address Translation (NAT) 6
6.5 Content analyzing and filtering 7

7 Security gateway components 7
7.1 Switches 7
7.2 Routers 8
7.3 Application Level Gateway 8
7.4 Security Appliances 8

8 Security Gateway Architectures 8
8.1 Structured approach 9
8.1.1 Packet filter firewall architecture 9
8.1.2 Dual-homed gateway architecture 10
8.1.3 Screened host architecture 11
8.1.4 Screened subnet architecture 12
8.2 Staged approach 13
8.2.1 Single and multi-staged security gateway architecture 14

9 Guidelines for selection and configuration 16
9.1 Selection of a security gateway architecture and appropriate components 17
9.2 Hardware and software platform 17
9.3 Configuration 17
9.4 Security features and settings 18
9.5 Administration 19
9.6 Logging 19
9.7 Documentation 20
9.8 Audit 20
9.9 Training and education 20
9.10 Miscellaneous 20

Bibliography 22