AS/NZS ISO/IEC 18028.3:2006
ISO/IEC 18028-3:2005

AS/NZS ISO/IEC 18028.3:2006

Australian/New Zealand Standard™

Information technology—Security techniques—IT network security

Part 3: Securing communications between networks using security gateways





Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006 and on behalf of the Council of Standards New Zealand on 30 June 2006.
This Standard was published on 4 August 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Department of Defence
Department of Social Welfare, NZ
Government Communications Security Bureau, NZ
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06259.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

Australian/New Zealand Standard™

Information technology—Security techniques—IT network security

Part 3: Securing communications between networks using security gateways

First published as AS/NZS ISO/IEC 18028.3:2006.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7668 X

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification.

The objective of this Standard is to provide detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. Those individuals within an organization that are responsible for IT security in general, and IT network security in particular, should be able to adapt the material in AS/NZS ISO/IEC 18028 series Standards to meet their specific requirements.

This Standard is Part 3 of the series and specifically defines techniques for securing for information flows between network using security gateway.

This Standard is identical with, and has been reproduced from ISO/IEC 18028-3:2005, *Information technology—Security techniques—IT network security*—Part 3: *Securing communications between networks using security gateways*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this part of ISO/IEC 18028' should read 'this Australian/New Zealand Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian/New Zealand Standard*	
ISO/IEC		AS ISO/IEC	
18028	Information technology—Security techniques—IT network security	18028	Information technology—Security techniques—IT network security
18028-4	Part 4: Securing remote access	18028.4	Part 4: Securing remote access

The term 'normative' has been used in this Standard to define the application of the appendix to which it applies. A 'normative' appendix is an integral part of a Standard.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

CONTENTS

Page

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

INTRODUCTION

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution. Thus, the purpose of ISO/IEC 18028 is to provide detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. Those individuals within an organization that are responsible for IT security in general, and IT network security in particular, should be able to adapt the material in ISO/IEC 18028 to meet their specific requirements. Its main objectives are as follows:

— in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security – including on how to identify and analyse the communications-related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);

— in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;

— in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;

— in ISO/IEC 18028-4, to define techniques for securing remote access;

— in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPN).

ISO/IEC 18028-1 is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for Information Security (IS) and/or network security, network operation, or who are responsible for an organization's overall security programme and security policy development.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example IT network managers, administrators, engineers and IT network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers, and IT network security officers).

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — IT network security —

Part 3:
Securing communications between networks using security gateways

1 Scope

This part of ISO/IEC 18028 provides an overview of different techniques of security gateways, of components and of different types of security gateway architectures. It also provides guidelines for selection and configuration of security gateways.

Although Personal Firewalls make use of similar techniques, they are outside the scope of this part of ISO/IEC 18028 because they do not serve as security gateways.

The intended audiences for this part of ISO/IEC 18028 are technical and managerial personnel, e.g. IT managers, system administrators, network administrators and IT security personnel. It provides guidance in helping the user choose the right type of architecture for a security gateway which best meets their security requirements.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
alert
'instant' indication that an information system and network may be under attack, or in danger because of accident, failure or people error

3.2
attacker
any person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

3.3
audit
formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity

3.4
audit logging
gathering of data on information security events for the purpose of review and analysis, and ongoing monitoring

3.5
Demilitarised Zone
DMZ
security host or small network (also known as a screened sub-net or a perimeter network) inserted as a 'neutral zone' between networks

NOTE It forms a security buffer zone.

cf. **security host**

3.6
filtering
process of accepting or rejecting data flows through a network, according to specified criteria

3.7
firewall
type of security barrier placed between network environments – consisting of a dedicated device or of a composite of several components and techniques – through which all traffic from one network environment to another, and vice versa, traverses and only authorized traffic, as defined by the local security policy, is allowed to pass

3.8
Information Security Incident
single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

NOTE See ISO/IEC 18044.

3.9
Information Security Incident Management
formal process of responding to and dealing with information security events and incidents

NOTE See ISO/IEC 18044.

3.10
Intrusion
unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system

3.11
Intrusion Detection
formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited to include how and when it occurred

3.12
Intrusion Detection System
IDS
technical system that is used to identify that an intrusion has been attempted, is occurring or has occurred, and possibly to respond to intrusions in IT systems and networks

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

3.13
port(1)
endpoint to a connection

3.14
port(2)
⟨internet protocol⟩ logical channel endpoint of a TCP or UDP connection

NOTE Application protocols which are based on TCP or UDP have typically assigned default port numbers, e.g. port 80 for the HTTP protocol.

3.15
privacy
the right of every individual that his/her private and family life, home and correspondence are treated confidentially, without interference by an authority except where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others

3.16
remote access
process of accessing network resources from another network, or from a terminal device which is not permanently connected to the network it is accessing

3.17
router
network device that is used to establish and control the flow of data between different networks, which themselves can be based on different network protocols, by selecting paths or routes based upon routing protocol mechanisms and algorithms

NOTE The routing information is kept in a routing table.

3.18
security dimension
set of security controls designed to address a particular aspect of network security

NOTE The detailed description of security dimensions is given in ISO/IEC 18028-2.

3.19
security domain
set of assets and resources subject to a common security policy

3.20
security gateway
point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy

NOTE A security gateway comprises more than only firewalls; the term includes routers and switches which provide the functionality of access control and optionally encryption.

3.21
spoofing
impersonating a legitimate resource or user

3.22
switch
device which provides connectivity between networked devices by means of internal switching mechanisms

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006

NOTE 1 Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point to point basis. This ensures the network traffic is only seen by the addressed network devices and enables several connections to exist simultaneously.

NOTE 2 Switching technology can be implemented at either layer 2 or layer 3 of the OSI reference model (ISO/IEC 7498-1)

3.23
Virtual Private Network
restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network

4 Abbreviated terms

API	Application Program Interface
BGP	Border Gateway Protocol
DLL	Dynamic Link Library
ICMP	Internet Control Message Protocol
IDP	Intrusion Detection Prevention
NFS	Network File Transfer
NIS	Network Information System
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SHTTP	Secure Hypertext Transfer Protocol
SOAP	Simple Object Access Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions protocol
SPAN	Switched Port Analyzer
TCP-SYN	Transmission Control Protocol, SYNchronisation
V.35	high-speed synchronous data exchange protocol
WAIS	Wide Area Information Service
X.11	graphical user interface protocol
XML	Extensible Mark-up Language

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.3-2006