

Australian/New Zealand Standard™

**Information technology—Security
techniques—IT network security**

**Part 5: Securing communications
across networks using virtual private
networks**



AS/NZS ISO/IEC 18028.5:2008

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 28 May 2008 and on behalf of the Council of Standards New Zealand on 31 May 2008. This Standard was published on 25 June 2008.

The following are represented on Committee IT-012:

Attorney General's Office
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Council of Small Business Organisations
Internet Industry Association
NSW Police
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 Standards may also be withdrawn.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 07260.

Australian/New Zealand Standard™

**Information technology—Security
techniques—IT network security**

**Part 5: Securing communications
across networks using virtual private
networks**

First published as AS/NZS ISO/IEC 18028.5:2008.

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 8765 7

PREFACE

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

The objective of this Standard is to provide IT professionals and general line management with detailed guidance on securing communications across networks using virtual private networks.

This Standard is identical with, and has been reproduced from ISO/IEC 18028-5:2006, *Information technology—Security techniques—IT network security, Part 5: Securing communications across networks using virtual private networks*.

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:

<i>Reference to International Standard</i>		<i>Australian/New Zealand Standard</i>	
ISO/IEC		AS/NZS	
17799	Information technology—Security Techniques—Code of practice for information security management	27002	Information technology—Security Techniques—Code of practice for information security management
		AS/NZS ISO/IEC	
18028	Information technology—Security techniques—IT network security	18028	Information technology—Security techniques—IT network security
18028-1	Part 1: Network security management	18028.1	Part 1: Network security management
18028-2	Part 2: Network security architecture	18028.2	Part 2: Network security architecture
18028-3	Part 3: Securing communications between networks using security gateways	18028.3	Part 3: Securing communications between networks using security gateways
18028-4	Part 4: Securing remote access	18028.4	Part 4: Securing remote access

Any international references not listed have not been adopted as Australian or Australian/New Zealand Standards.

The term ‘informative’ has been used in this Standard to define the application of the appendix to which it applies. An ‘informative’ appendix is only for information and guidance.

CONTENTS

Page

1	Scope	1
2	Normative references	1
3	Terms and definitions	2
3.1	Terms defined in other International Standards.....	2
3.2	Terms defined in this part of ISO/IEC 18028	2
4	Abbreviated terms	3
5	Overview of VPNs	3
5.1	Introduction	3
5.2	Types of VPN	4
5.3	VPN techniques.....	5
5.4	Security aspects	6
6	VPN security objectives	7
7	VPN security requirements	7
7.1	Confidentiality	8
7.2	Integrity	8
7.3	Authentication	8
7.4	Authorization	8
7.5	Availability	8
7.6	Tunnel Endpoints.....	8
8	Guidelines for the selection of secure VPNs	9
8.1	Regulatory and legislative aspects	9
8.2	VPN management aspects	9
8.3	VPN architectural aspects	9
9	Guidelines for the implementation of secure VPNs	12
9.1	VPN management considerations.....	12
9.2	VPN technical considerations	12
	Annex A (informative) Technologies and protocols used to implement VPNs.....	15
A.1	Introduction	15
A.2	Layer 2 VPNs	15
A.3	Layer 3 VPNs	17
A.4	Higher Layer VPNs.....	17
A.5	Comparison of typical VPN protocol security features	19
	Bibliography	20

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 information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and 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 analyze 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 (VPNs).

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 and/or network security, network operation, or who are responsible for an organization's overall security program 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 network managers, administrators, engineers, and 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 network managers, administrators, engineers and 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 network managers, administrators, engineers, and 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 network managers, administrators, engineers, and network security officers).

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — IT network security —**Part 5:****Securing communications across networks using virtual private networks****1 Scope**

This part of ISO/IEC 18028 provides detailed direction with respect to the security aspects of using Virtual Private Network (VPN) connections to inter-connect networks, and also to connect remote users to networks. It builds upon the network management direction provided in ISO/IEC 18028-1.

It is aimed at those individuals responsible for the selection and implementation of the technical controls necessary to provide network security when using VPN connections, and for the subsequent network monitoring of VPN security thereafter.

This part of ISO/IEC 18028 provides an overview of VPNs, presents VPN security objectives, and summarizes VPN security requirements. It gives guidance on the selection of secure VPNs, on the implementation of secure VPNs, and on the network monitoring of VPN security. It also provides information on typical technologies and protocols used by VPNs.

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 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18028-1:2006, *Information technology — Security techniques — IT network security — Part 1: Network security management*

ISO/IEC 18028-2:2006, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

3 Terms and definitions

3.1 Terms defined in other International Standards

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts) and ISO/IEC 18028-1 apply, as do the following terms defined in ISO/IEC 13335-1: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, security policy, non-repudiation, reliability, risk, risk analysis, risk management, safeguard, threat, and vulnerability.

3.2 Terms defined in this part of ISO/IEC 18028

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

3.2.1

layer 2 switching

technology that uses internal switching mechanisms to establish and control connections between devices using layer 2 protocols

NOTE It is typically used to simulate a LAN environment to upper layer protocols.

3.2.2

layer 2 VPN

virtual private network used to provide a simulated LAN environment over a network infrastructure

NOTE Sites linked by a layer 2 VPN can operate as though they are on the same LAN.

3.2.3

layer 3 switching

technology that uses internal switching mechanisms in combination with standard routing mechanisms, or which employs MPLS techniques, in order to establish and control connections between networks

3.2.4

layer 3 VPN

virtual private network used to provide a simulated WAN environment over a network infrastructure

NOTE Sites linked by a layer 3 VPN can operate as though they are on a private WAN.

3.2.5

private

restricted to members of an authorized group: in the context of VPNs, it refers to the traffic flowing in a VPN connection

3.2.6

private network

network that is subject to access controls which are intended to restrict use to members of an authorized group

3.2.7

protocol encapsulation

enveloping one data flow inside another by transporting protocol data units wrapped inside another protocol

NOTE This is one method which can be used to establish tunnels in VPN technology.

3.2.8**virtual circuit**

data path between network devices established using a packet or cell switching technology such as X.25, ATM or Frame Relay

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 18028-1 and the following apply.

AH	Authentication Header
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IPX	Internetwork Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
L2F	Layer Two Forwarding (Protocol)
L2TP	Layer 2 Tunneling Protocol
LDP	Label Distribution Protocol
MPPE	Microsoft Point-to-Point Encryption
NAS	Network Area Storage
NCP	Point-to-Point Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
SSL	Secure Sockets Layer
VPLS	Virtual Private LAN Service
VPWS	Virtual Private Wire Service

5 Overview of VPNs**5.1 Introduction**

VPNs have developed rapidly as a means of inter-connecting networks, and as a method of connecting remote users to networks. A VPN is an example of a type of technology that can implement the Communication Flow Security Dimension described in ISO/IEC 18028-2, the security for which is considered as part of the Services Security Layer (as defined in ISO/IEC 18028-2).

There exists a broad range of definitions for VPNs. In their simplest form, they provide a mechanism for establishing a secure data channel or channels over an existing network or point-to-point connection. They are assigned to the exclusive use of a restricted user group, and can be established and removed dynamically, as needed. The hosting network may be private or public.

An example representation of a VPN, with the secure data channel connecting the two endpoints across an insecure public network, is shown in Figure 1 below.

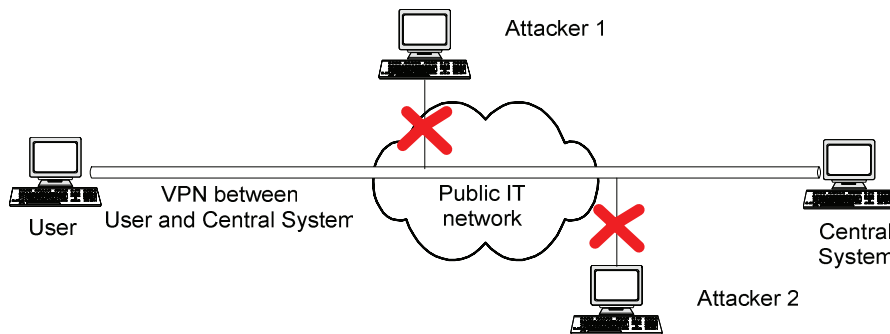


Figure 1 — Example representation of a VPN

Remote access using a VPN is implemented over the top of a normal point-to-point connection, which should first be established between the local user and the remote location in line with ISO/IEC 18028-4. The connection could take the form of wired or wireless network technology.

Some VPNs are provided as a managed service, in which secure, reliable connectivity, management and addressing, equivalent to that on a private network, are provided on a shared infrastructure. Additional security controls, as indicated in this standard, may therefore need to be taken into account to strengthen the VPN.

The data and code transiting a VPN should be restricted to the organization using the VPN and should be kept separate from other users of the underlying network. It should not be possible for data and code belonging to other users to access the same VPN channel. The level of trust in the confidentiality and other security aspects of the organization owning or providing the VPN should be taken into consideration when evaluating the extent of additional security controls that may be required.

5.2 Types of VPN

As stated above, there are multiple ways of expressing types of VPN.

Architecturally, VPNs comprise either:

- a single point-to-point connection (e.g. client device remotely accessing an organization's network via a site gateway, or a site gateway connecting to another site gateway), or
- a point-to-cloud connection (e.g. implemented by MPLS technology).

From an OSI Basic Reference Model perspective, there are three main types of VPN:

- Layer 2 VPNs offer a simulated LAN facility, using VPN connections running over a hosting network (e.g. a provider's network) to link sites of an organization or to provide a remote connection to an organization. Typical provider offerings in this area include Virtual Private Wire Service (VPWS), which provides a simulated "wires only connection", or Virtual Private LAN Service (VPLS), which provides a more complete simulated LAN service.
- Layer 3 VPNs offer a simulated WAN facility, again using VPNs running over a network infrastructure. These offerings provide sites with simulated "OSI Network Layer" connectivity. A basic attraction here is the ability to use private IP addressing schemes over a public infrastructure, a practice that would not be permitted over a "normal" public IP connection. Whilst private addresses can be used over public networks via NAT (Network Address Translation), this can complicate IPsec VPN establishment and use, although there are work-arounds available.