BS ISO/IEC 27033-4:2014

BSI Standards Publication

Information technology — Security techniques — Network security

Part 4: Securing communications between networks using security gateways

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 27033-4:2014

National foreword

This British Standard is the UK implementation of ISO/IEC 27033-4:2014. It supersedes BS ISO/IEC 18028-3:2005 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 65101 4

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-4:2014

INTERNATIONAL STANDARD

ISO/IEC 27033-4

First edition
2014-03-01

Information technology — Security techniques — Network security —

Part 4: Securing communications between networks using security gateways

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

Partie 4: Sécurisation des communications entre réseaux en utilisant des portails de sécurité

Reference number
ISO/IEC 27033-4:2014(E)

Documents
Document Sharing Hub
© ISO/IEC 2014

Full document details: BS ISO/IEC 27033-4:2014

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-4:2014

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **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**

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-4:2014

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27033-4 cancels and replaces ISO/IEC 18028-3:2005, which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios – Threats, design techniques and control issues*

— *Part 4: Securing communications between networks using security gateways*

— *Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*

— *Part 6: Securing wireless IP network access*

(Note that there may be other Parts. Examples of possible topics to be covered by Parts include local area networks, wide area networks, broadband networks, web hosting, Internet email, and routed access to third party organizations. The main clauses of all such Parts should be Risks, Design Techniques and Control Issues.)

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-4:2014

Introduction

The majority of both commercial and government organizations have their information systems connected by networks, with the network connections being one or more of the following:

— within the organization.

— between different organizations.

— between the organization and the general public.

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet Service Providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Further, the new technology (including the integration of data, voice and video) increases the opportunities for remote working (also known as teleworking or telecommuting). Telecommuters are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, while this environment does facilitate significant business benefits, there are new security threats to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major need to properly protect networks and their related information systems and information. In other words, implementing and maintaining adequate network security is critical to the success of any organization's business operations.

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, thereby meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential to achieve accurate billing for network usage. 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 security solution.

The purpose of ISO/IEC 27033-4, Securing communications between networks using security gateways, is to provide guidance on how to identify and analyse network security threats associated with security gateways, define the network security requirements for security gateways based on threat analysis, introduce design techniques to achieve a network technical security architecture to address the threats and control aspects associated with typical network scenarios, and address the issues associated with implementing, operating, monitoring and reviewing network security controls with security gateways.

It is emphasized that the ISO/IEC 27033-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network architects and designers, network managers, and network security officers).

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-4:2014

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-4:2014

INTERNATIONAL STANDARD ISO/IEC 27033-4:2014(E)

Information technology — Security techniques — Network security —

Part 4: Securing communications between networks using security gateways

1 Scope

This part of ISO/IEC 27033 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with a documented information security policy of the security gateways, including:

a) identifying and analysing network security threats associated with security gateways;

b) defining network security requirements for security gateways based on threat analysis;

c) using techniques for design and implementation to address the threats and control aspects associated with typical network scenarios; and

d) addressing issues associated with implementing, operating, monitoring and reviewing network security gateway controls.

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 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27033-1 and the following apply.

3.1
bastion host
specific host with hardened operation system that is used to intercept packets entering or leaving a network and the system that any outsider must normally connect with to access a service or a system that lies within an organization's firewall

3.2
end-point software-based firewall
software application running on a single machine, protecting network traffic into and out of that machine to permit or deny communications based on an end user-defined security policy

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-4:2014

3.3
hardened operating system
operating system which has been configured or designed specifically to minimize the potential for comprise or attack

Note 1 to entry: This may be a general OS, such as Linux, which has been configured for this environment or may be a more custom built solution.

3.4
Internet gateway
entry point to access the internet

3.5
packet
entity comprising a well-defined block of bytes consisting of 'header', 'data' and optional 'trailer' which can be transmitted across networks or over telephone lines

Note 1 to entry: The format of a packet depends on the protocol that created it. Various communications standards and protocols use special purpose packets to monitor and control a communications session. For example the X.25 standard uses diagnostic, call clear and reset packets (among others), as well as data packets (or) a unit of data that is transmitted over the network.

3.6
perimeter network
physical or logical subnetwork that contains and exposes an organization's external services to a public network

3.7
remote office
branch office
office externally connected to the organization's main office through remote networks to provide users with services (e.g. file, print and the other service) required to maintain their daily business routine

3.8
single point of failure
type of failure that if a part of a system fails, the entire system does not work

3.9
SIP gateway
perimeter device that sits between the internal VoIP network and an external network such as the public telephone network

Note 1 to entry: Often a router is used to perform the role. Where VoIP is in use to external IP networks it is important to ensure that the gateway contains sufficient security measures especially dynamic rule base changes to all call setup to take place securely.

4 Abbreviated terms

ACL	Access Control List
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
CPU	Central Processing Unit
DDoS	Distributed Denial-of-Service

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-4:2014

DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoS	Denial-of-Service
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NFS	Network File System
NIS	Network Information System
NNTP	Network News Transport Protocol
NTP	Network Time Protocol
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SIP	Session Initiation Protocol
SMS	Short Message Service
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPA	Switched Port Analyzer
SPOF	Single Point Of Failure
SQL	Structured Query Language

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-4:2014