ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 25068.2-2020

Replacing GB/T 25068.2-2012

Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security

Issued on: November 19, 2020 **Implemented on: June 1, 2021**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Foreword

GB/T 25068 "Information Technology Security Technology Cyber Security" is currently divided into the following 5 parts:

---Part 1: Overview and concepts;

---Part 2: Network Security Design and Implementation Guidelines;

---Part 3: Reference network scenarios---risk, design technology and control elements;

---Part 4: Security Protection of Internet Communication Using Security Gateway;

---Part 5: Security protection of cross-network communication using virtual private network:

This part is Part 2 of GB/T 25068:

This section was drafted in accordance with the rules given in GB/T 1:1-2009:

This part replaces GB/T 25068:2-2012 "Information Technology Security Technology IT Cyber Security Part 2: Cyber Security System

Structure", compared with GB/T 25068:2-2012, the main technical changes are as follows:

--- Deleted "Network Security Reference Architecture", "Security Maintenance", "Security Layer", "Security Surface", "Security Threats", and "Apply to Security Maintenance"

Contents such as the description of the goals achieved at the entire level have been added, including the "document structure", "network security design preparation", "network security design", and "network security design":

Network Security Implementation" and other content (see Chapter 5~Chapter 8,:2012 Edition Chapter 5~Chapter 10);

---Modified the content of the scope of Chapter 1 (see Chapter 1, Chapter 1 of the:2012 edition);

---Delete the reference of the normative reference document GB/T 9387:2-1995, add ISO /IEC 27000:2009, ISO /IEC

27001:2005, ISO /IEC 27002:2005, ISO /IEC 27005:2011, ISO /IEC 7498 (all parts), ISO /

Reference to IEC 27033-1 (see Chapter 2, Chapter 2 of the:2012 edition);

--- Delete the terms and definitions in Chapter 3, and modify the introductory language (see Chapter 3, Chapter 3 of the:2012 edition);

--- Deleted "ASP" "ATM" "DHCP" "DNS" "DS-3" "Ipsec" "MD5" "Megaco/H:248" "MPLS"

"OAM

Abbreviations such as "SSL", "VLAN", etc:, and abbreviations such as "IPS", "POC", "RADIUS", "SMS", "TACACS", and "TFTP" have been added

Language (see Chapter 4, Chapter 4 of the:2012 edition):

The translation method used in this part is equivalent to ISO /IEC 27033-2:2012 "Information Technology Security Technology Cyber Security Part 2

Sub: Network Security Design and Implementation Guide:

The Chinese documents that have a consistent correspondence with the international documents cited in this section are as follows:

---GB/T 9387 (all parts) Information Technology Open System Interconnection Basic Reference Model [ISO /IEC 7498 (all parts)

Points), IDT];

---GB/T 22080-2016 Information technology security technology information security management system requirements (ISO /IEC 27001:

2013, IDT);

---GB/T 22081-2016 Information Technology Security Technical Information Security Control Practice Guide (ISO /IEC 27002:2013,

IDT);

---GB/T 25068:1-2020 Information Technology Security Technology Cyber Security Part 1: Overview and Concepts (ISO /IEC

27033-1:2015, IDT);

---GB/T 29246-2017 Information Technology Security Technology Information Security Management System Overview and Vocabulary (ISO /IEC

27000:2016, IDT);

---GB/T 31722-2015 Information Technology Security Technology Information Security Risk Management (ISO /IEC 27005:2008,

IDT):

This part is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260):

Drafting organizations of this part: Heilongjiang Provincial Cyberspace Research Center, China Electronic Technology Standardization Institute, Beijing Antiy Cyber Security Technology

Technology Co:, Ltd:, Hangzhou Anheng Information Technology Co:, Ltd:, Harbin University of Science and Technology, Xi'an Xidian Jietong Wireless Network Communication Co:, Ltd:

1 Scope

This part of GB/T 25068 gives organizations guidelines for planning, designing, implementing and documenting network security:

2 Normative references

The following documents are indispensable for the application of this document: For dated reference documents, only the dated version applies to this article

Pieces: For undated references, the latest version (including all amendments) applies to this document:

ISO /IEC 7498 (all parts) Information Technology Open System Interconnection Basic Reference Model (Informationtechnology-

Opensystemsinterconnection-Basicreferencemodel)

ISO /IEC 27000:2009 Information Technology Security Technology Information Security Management System Overview and Vocabulary (Information

technology-Securitytechniques-Informationsecuritymanagementsystems-Overviewandvocabu-

lary)

ISO /IEC 27001:2005 Information Technology Security Technology Information Security Management System Requirements (Informationtechnology-

Securitytechniques-Informationsecuritymanagementsystems-Requirements)

ISO /IEC 27002:2005 Information Technology Security Technology Information Security Management Practical Rules (Informationtechnology-

Securitytechniques-Codeofpracticeforinformationsecuritymanagement)

ISO /IEC 27005:2011 Information Technology Security Technology Information Security Risk Management (Informationtechnology-Secu-

ritytechniques-Informationsecurityriskmanagement)

ISO /IEC 27033-1 Information Technology Security Technology Cyber Security Part 1: Overview and Concepts (Informationtech-

nology-Securitytechniques-Networksecurity-Part 1:Overviewandconcepts)

3 Terms and definitions

ISO /IEC 7498 (all parts), ISO /IEC 27000:2009, ISO /IEC 27001:2005, ISO /IEC 27002:2005,

The terms and definitions defined by ISO /IEC 27005:2011 and ISO /IEC 27033-1 apply to this document:

4 Abbreviations

The following abbreviations apply to this document:

IPS: Intrusion Prevention System (Intrusion Prevention System)

POC: Proof of Concept (ProofofConcept)