ICS 35.030
CCS L 80

# NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA



# GB/T 25068.4-2022

Replacing GB/T 25068.3-2010

# Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways

**Issued on: October 14, 2022** **Implemented on: May 1, 2023**

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

# Table of Contents





## foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1.Structure and Drafting Rules of Standardization Documents"

drafted.

This document is part 4 of GB/T 25068 "Information Technology Security Technology Network Security". GB/T 25068 has been published with

the next part.

--- Part 1.Overview and concepts;

--- Part 2.Guidelines for network security design and implementation;

--- Part 3.Threats, design techniques and controls for network access scenarios;

--- Part 4.Security protection of inter-network communication using security gateways;

--- Part 5.Cross-network communication security protection using virtual private network.

This document replaces GB/T 25068.3-2010 "Information Technology Security Technology IT Network Security Part 3.Using Security Gateways"

Internet Communication Security Protection. Compared with GB/T 25068.3-2010, except for structural adjustment and editorial changes, the main technical changes

as follows.

a) Changed the recommended terms and expressions used when stating "scope" (see Chapter 1, Chapter 1 of the.2010 edition);

b) Changed the content of "Terms and Definitions" (see Chapter 3, Chapter 3 of the.2010 edition);

c) Deleted abbreviations such as "IT", "IDP", "V.35", and added abbreviations such as "ACL", "ASIC", "CPU", "DDoS" and "URL"

(See Chapter 4, Chapter 4 of the.2010 edition);

d) Added three chapters "Document Structure", "Overview" and "Security Threats" (see Chapters 5 to 7);

e) Changed "Security Requirements" to "Security Requirements", added "Table 1", and incorporated the relevant contents of the.2010 edition after changes (see Section 1.1).

Chapter 8, Chapter 5 of the.2010 edition);

f) Changed "Security Gateway Technology" to "Security Control" (see Chapter 9, Chapter 6 of the.2010 edition), and added the element "General" (see Chapter 6 of the.2010 edition)

9.1), "Intrusion Prevention System and Intrusion Detection System" (see 9.6), "Security Management API" (see 9.7), deleted the element "Network location".

Address Translation (NAT)" (see 6.4 of the.2010 edition);

g) Deleted the comparison of the advantages and disadvantages of "Stateful Packet Inspection Firewall" and "Application Proxy Firewall", and changed the relevant content of the.2010 edition to

Incorporated after modification (see 9.3, 6.2 of the.2010 edition);

h) Changed "Application Proxy" to "Application Firewall", and incorporated the relevant content of the.2010 version after the modification (see 9.4,.2010 version

6.3);

i) Changed "Content Analysis and Filtering" to "Content Filtering", added "Content Analysis" column item "Protocol Analysis", and changed the.2010 version

The relevant content is changed and incorporated (see 9.5, 6.5 of the.2010 edition);

j) The chapters "Security Gateway Components" and "Security Gateway Architecture" were merged into the "Design Techniques" chapter, and the dangling segment guidance was deleted

Words, redrawn the schematic diagram (see Figure 3 to Figure 6, Figure 1 to Figure 4 of the.2010 edition), and changed the relevant content of the.2010 edition

later included (see Chapter 10, Chapters 7 and 8 of the.2010 edition);

k) Added the usage rule of "There may be a load balancing switch" (see 10.1.1, 7.1 of the.2010 edition);

l) Changed "application-level gateway" to "application-level gateway", added the usage rules of "SIP gateway", and changed the relevant rules of the.2010 edition

Incorporated after content changes (see 10.1.3, 7.3 of the.2010 edition);

m) Added the usage rules of "monitoring function" (see 10.1.5);

n) Changed "Security Gateway Architecture" to "Deploying Security Gateway Controls", removed the overhang section (see 10.2,.2010 edition of

8.1);

o) Deleted the element "Hierarchical approach" (see 8.2 of the.2010 edition);

p) deleted the paragraph describing the advantages and disadvantages of "shielded host architecture" (see 8.1.3 of the.2010 edition);

q) Added the usage rules of "Packet Filtering Firewall" (see 10.2.1);

r) Added the element "General" (see 11.1);

s) Changed "Security Features and Settings" to "Security Features Settings", added "Support for packaged enterprise or other business applications"

Proxy Services" and "Support for identifying applications running in protocol streams (such as office productivity applications, embedded video, instant messaging, etc.)"

The recommended clauses of the.2010 edition will be incorporated into the revised version (see 11.5, 9.4 of the.2010 edition);

t) Added "fine-grained access rights" (see 11.6, 9.6 of the.2010 edition);

u) deleted the element "documentation" (see 9.7 of the.2010 edition);

v) elements "implementation type" and elements "high availability and operation mode" were added (see 11.10, 11.11).

This document is equivalent to ISO /IEC 27033-4.2014 "Information Technology Security Technology Cybersecurity Part 4.Security of Use"

Internet Communication Security Protection of Gateways.

The following minimal editorial changes have been made to this document.

--- Replaced ISO /IEC 27035 (see 9.1) with GB/T 20985.2-2020 cited for information;

--- Replaced ISO /IEC 27039 (see 9.5) with GB/T 28454-2020 cited for information;

Please note that some content of this document may be patented. The issuing agency of this document assumes no responsibility for identifying patents.

## Introduction

The purpose of GB/T 25068 is to provide detailed guidance on the security aspects of the management, operation, use and interconnection of information system networks.

To facilitate the adoption of this document by those responsible for information security,

especially cybersecurity, within the organization to meet their specific needs. to consist of six parts

constitute.

--- Part 1.Overview and concepts. The purpose is to define and describe concepts related to cybersecurity and to provide management guidance.

--- Part 2.Network security design and implementation guidelines. The purpose is to help organizations plan, design, and implement high-quality cybersecurity

system to ensure that network security is suitable for the appropriate business environment to provide guidance.

--- Part 3.Threats, design techniques and controls for network access scenarios. The purpose is to enumerate typical network access scenarios

The specific risks, design techniques, and controls related to cybersecurity are applicable to all those involved in the planning, design, and implementation of cybersecurity architecture.

--- Part 4.Security protection of inter-network communication using security gateways. The purpose is to secure Internet-to-network communications using a secure gateway.

It provides information on how to identify and analyze network security threats related to security gateways, and define a network security gateway based on threat analysis.

Network security requirements, introduces network technology security architecture design techniques to address threats and controls associated with typical network scenarios

Guidelines for technical implementation and addressing issues related to the use of secure gateways to implement, operate, monitor, and review network security controls. This article

This software applies to all those involved in the detailed planning, design and implementation of security gateways (e.g. network architects and designers, network

administrators and cybersecurity executives).

--- Part 5.Cross-network communication security protection using virtual private network. The purpose is to define the use of virtual private networks to establish secure connections

The specific risks, design techniques and control elements that are involved.

--- Part 6.Wireless network access security. The purpose is to provide for the selection, implementation and monitoring of the use of wireless networks necessary to provide secure communications

The technical controls of the

Check and select.

GB/T 25068 is based on GB/T 22081 "Information Technology Security Technology