Chinastandards.org

ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 25068.7-2025

Information technology - Security techniques - Network security - Part 7: Network virtualization security

信息技术 安全技术 网络安全 第7部分：网络虚拟化安全

(English Translation)

Issued on: December 2, 2025 **Implemented on: July 1, 2026**

Issued by: State Administration for Market Regulation

Preview: page 1 of 5 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25068-7-2025

Chinastandards.org

Table of Contents

Preface
Introduction
1 Scope
2 Normative References
3 Terms and Definitions
4 Abbreviations
5 Overview
5.1 Overview
5.2 Description of Network Virtualization
5.3 Security Model
5.3.1 Network Virtualization Security Model
5.3.2 Network Virtualization Components
6 Security Threats
7 Safety Recommendations
7.1 Overview
7.2 Confidentiality
7.3 Integrity
7.4 Availability
7.5 Identity Authentication
7.6 Access Control
7.7 Non-repudiation
8 Safety Controls
8.1 Overview
8.2 Security of Virtual Network Infrastructure
8.3 Virtual Network Functional Safety
8.4 Virtual Network Management Security
8.4.1 SDN Controller Security
8.4.2 NFV Orchestrator Security
9 Safety Design and Considerations
9.1 Overview
9.2 Platform Integrity Protection
9.3 Enhanced Network Virtualization

Preview: page 2 of 5 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25068-7-2025

9.4 API Authentication and Authorization

9.5 Software-defined security for virtual networks

Appendix A (Informative) Network Virtualization Application Case

A.1 Software-Defined Wide Area Networks

A.2 Network Slicing

A.3 vWAF

A.4 Cloud CDN with centralized control function

Appendix B (Informative) Detailed Description of Security Threats to Network Virtualization

B.1 Security Threats to Virtual Network Infrastructure

B.2 Virtual Network Functional Security Threats

B.2.1 Virtual Network Functional Security Threats

B.2.2 Software-Defined Network Security Threats

B.3 Virtual Network Management Security Threats

B.3.1 Overview

B.3.2 Software-Defined Network Controller Security

B.3.3 Management and scheduling security

B.3.4 Interface Security

B.4 Threats of Specific Virtualizations

B.4.1 Network Segmentation Threat

B.4.2 Threat of Resource Depletion

B.4.3 Centralized Threat Management

Reference

Foreword

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

Drafting.

This document is Part 7 of GB/T 25068 "Information Technology Security Technology - Network Security". GB/T 25068 has been published as follows.

Part 2.

---Part 1: Overview and Concepts;

---Part 2: Guidelines for Cybersecurity Design and Implementation;

Preview: page 3 of 5 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25068-7-2025

---Part 3: Threats, Design Techniques, and Controls for Network Access Scenarios;

---Part 4: Security Protection for Internet Communication Using Security Gateways;

---Part 5: Security Protection for Cross-Network Communication Using Virtual Private Networks;

---Part 6: Wireless Network Access Security;

---Part 7: Network Virtualization Security.

This document is equivalent to ISO/IEC 27033-7:2023 "Information technology - network security - Part 7.security of network virtualization".

guide".

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

---To align with existing standards, the standard name has been changed to "Information Technology Security Technology. Network Security Part 7: Virtual Networks".

"Simulated Security"

---Added abbreviations such as "ACL", "AR", "eMTC", and "IT" (see Chapter 4);

---Added a note to the content described in Figure 1 (see 5.3.1);

---Added notes for "Bare Metal Architecture", "Host Architecture", "Southbound Interface", and "Northbound Interface" (see 5.3.2 and 8.3);

---Added notes to the contents described in Table 1 (see 7.7);

---Added a note regarding the applicability of GM/T 0068-2019 (see 9.4).

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260).

Introduction

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

This standard is designed to facilitate the adoption of security-related personnel (e.g., cybersecurity personnel) within organizations to meet their specific needs. GB/T 25068 comprises seven departments.

The structure is divided into several parts, and the main objectives of each part are as follows.

Preview: page 4 of 5 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25068-7-2025

---Part 1: Overview and Concepts. Defines and describes concepts related to cybersecurity and provides management guidance.

---Part 2: Guidelines for Cybersecurity Design and Implementation. Provides organizations with guidance on how to plan, design, and implement high-quality cybersecurity architectures.

Provide guidance.

---Part 3: Threats, Design Techniques, and Controls for Network Access Scenarios. This section lists specific threats, design techniques, and controls relevant to typical network access scenarios.

Body risk, design technology and control.

---Part 4: Security Protection for Inter-network Communication Using Security Gateways. Provides guidance on the implementation, operation, monitoring, and auditing of network security using security gateways.

Guidelines on issues related to full control.

---Part 5: Security Protection for Cross-Network Communication Using Virtual Private Networks. Defines the specific measures for establishing secure connections using Virtual Private Networks.

Body risk, design technology and control elements.

---Part 6: Wireless Network Access Security. Defines the specific risks, design techniques, and controls for secure communication using wireless networks.

Elements, providing guidance for selecting, implementing, and monitoring the technical controls necessary for secure communications using wireless networks, applicable to all There are personnel involved in the detailed planning, design, and implementation of wireless network security.

---Part 7: Network Virtualization Security. Identifying network virtualization security risks and providing solutions for the secure implementation of network virtualization.

Guidelines.

It should be emphasized that GB/T 25068 provides more detailed implementation guidelines for network security controls, while GB/T 22081 addresses the aforementioned network...

The network security control has been described in a basic standardized manner.

Information technology security technology network security Part 7: Network Virtualization Security

Preview: page 5 of 5 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gb-t-25068-7-2025