

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 25068.5-2021

**Information technology - Security techniques - Network
security - Part 5: Securing communications across networks
using virtual private networks**

信息技术 安全技术 网络安全 第5部分：使用虚拟专用网的跨网通信安全保护
(English Translation)

Issued on: March 9, 2021

Implemented on: October 1, 2021

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

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Overview	
5.1 Introduction	
5.2 VPN Type	
6 Security threat	
7 Safety requirements	
7.1 Overview	
7.2 Confidentiality	
7.3 Completeness	
7.4 Identification	
7.5 Authorization	
7.6 Usability	
7.7 Tunnel Endpoint Security	
8 Security Control	
8.1 Safety aspects	
8.2 Virtual Circuit	
9 VPN related technologies	
9.1 Overview	
9.2 Regulations and legal aspects	
9.3 VPN management aspects	
9.4 VPN architecture aspects	
9.4.1 Overview	
9.4.2 Endpoint Security	
9.4.3 End point security	
9.4.4 Malware protection	
9.4.5 Identification	
9.4.6 Intrusion Detection and Defense System	
9.4.7 Security Gateway	

- 9.4.8 Network Design
- 9.4.9 Other connections
- 9.4.10 Separation tunnel
- 9.4.11 Log audit and network monitoring
- 9.4.12 Management of technical vulnerabilities
- 9.4.13 Public network routing encryption
- 9.5 VPN Technical Considerations
 - 9.5.1 Background
 - 9.5.2 VPN device management
 - 9.5.3 VPN security monitoring
- 10 Product Selection Guide
 - 10.1 Choice of bearer protocol
 - 10.2 VPN device
- Appendix A (informative appendix) TISec technology
- Reference

1 Scope

This part of GB/T 25068 specifies the use of virtual private network (VPN) to connect to the Internet and connect remote users to the network.

Security requirements, and guidelines for the selection, implementation and monitoring of control technologies necessary for using VPN to provide network security.

This section applies to those responsible for selecting and implementing technical control personnel necessary to provide network security when using VPNs, as well as subsequent VPN security network monitoring personnel.

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 reference documents, the latest version (including all amendments) is applicable to this document.

GB/T 9387 (all parts) Open System Interconnection Basic Reference Model [ISO 7498 (all parts)]

GB/T 17901.1-2020 Information Technology Security Technology Key Management Part 1: Framework (ISO /IEC 11770-1. 2010, MOD)

GB/T 22080-2016 Information Technology Security Technology Information Security Management System Requirements (ISO /IEC 27001:2013, IDT)

GB/T 22081 Information Technology Security Technical Information Security Control Practice Guide (GB/T 22081-2016, 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 31722-2015 Information Technology Security Technology Information Security Risk Management (ISO /IEC 27005:2008, IDT)

3 Terms and definitions

GB/T 9387 (all parts), GB/T 22080-2016, GB/T 22081, GB/T 25068.1-2020, GB/T 31722- The terms and definitions defined in 2015 and the following apply to this document.

3.1 Private

Limited to authorized users.

3.2 Tunnel

Between networked devices, the data path hidden in other protocols with higher visibility.

3.3 Virtual private network

Based on physical network system resources, a restricted-use virtual network constructed through tunneling technology.

3.4 Virtual circuit

Data channels between network devices established using packet or cell switching technologies such as X.25, ATM, or Frame Relay.

3.5 Protocol encapsulation

By transmitting the protocol data unit wrapped in another protocol, one data stream is encapsulated in another data stream.

Note: This method can be used to establish tunnels in virtual private network technology.

5.1 Introduction

As a method of network interconnection and a method of connecting remote users to the network, VPN technology has been developing rapidly.

There is a wide range of VPN definitions. According to its simplest definition, VPN provides

a way to connect to existing networks or peer-to-peer Connect to the mechanism of establishing one or more secure data channels. It is only allocated to restricted user groups for exclusive use, and can be dynamically built when needed.

Establish and revoke. The host network can be private or public.

The schematic diagram of VPN is shown in Figure 1. It has a cross-domain public network to connect the secure data channel of the endpoint and gateway, and a cross-domain public network.

The public network is used to connect the secure data channels of the two gateways.

Remote access using VPN is realized on top of ordinary point-to-point connection. First, establish a connection between the local user and the remote location Establish an ordinary point-to-point connection. Some VPNs are provided as a managed service. In these VPNs, secure and reliable connectivity, Management and addressing functions (the same as those on the private network) are provided on a shared infrastructure. The additional security given in this section can be used Control to enhance VPN functions.

The data and codes that traverse the VPN should be restricted to the organization that uses the VPN, and should be kept separate from other users of the underlying network.

Data and codes belonging to other users should not have the ability to access the same VPN channel. When the scope of additional security controls may need to be evaluated At the same time, the credibility of the organization that owns or provides the VPN in terms of confidentiality and other security should be considered.

5.2 VPN type

As mentioned above, there are many ways to express VPN. From an architectural perspective, VPN includes.

---Single point-to-point connection (for example, the client accesses the organization network remotely via the site gateway, or the site gateway connects to another Site gateway);

--- Point-to-cloud connection (for example, implemented through MPLS technology).

From the perspective of the OSI basic reference model, there are three main types of VPNs.

---Layer 2 VPN provides simulated LAN facilities. It uses a VPN running on the host network (e.g. provider network)

Connect to link the organization's site or provide a remote connection to the organization. Typical providers in this field usually provide virtual private Line Service (VPWS) or Virtual Local Area Network Service (VPLS). Among them, VPWS provides a virtual "wired connection", VPLS Provide a more complete analog LAN service.