ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 31499-2026

Replacing GB/T 31499-2015

Cybersecurity technology - Technical specification for unified threat management products

网络安全技术 统一威胁管理产品（UTM）技术规范

Issued on: April 30, 2026 **Implemented on: November 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

6.1.1 Access Control

6.1.1.1 Bandwidth Management The product should have bandwidth management functionality, with the following requirements.

a) Supports limiting traffic to a specified value based on conditions such as source IP address, destination IP address, protocol, application type, and time;

b) Supports bandwidth guarantees, ensuring that in the event of congestion, the stream will be re-encoded for a specified source IP address, destination IP address, protocol, application type, and time. The data is prioritized and forwarded according to a pre-set strategy.

6.1.1.2 Network Layer Access Control The product should have network layer access control functionality, with the following requirements.

a) The security policy uses the principle of least security, meaning that it prohibits anything

unless explicitly permitted;

b) The security policy includes access control based on source IP address, destination IP address, transport protocol, source port, and destination port;

c) The security policy includes MAC address-based access control;

d) The security policy includes time-based access control;

e) Supports user-defined security policies, including MAC address, IP address, port, transport protocol, and time information. Or all combinations;

f) Supports automatic or manual binding of IP and MAC addresses. When the host's IP address and MAC address are bound to the IP/MAC address binding table... If there is a discrepancy, prevent its flow from passing through.

6.1.1.3 Application Layer Access Control The product should have application-layer access control functionality, with the following requirements.

a) Supports user authentication-based access control functions, including local user authentication and integration with third-party authentication systems;

b) Supports URL-based access control and includes a URL classification library;

c) Supports file type detection and filtering based on common protocols such as FTP, HTTP, HTTPS, POP3, IMAP, and SMTP. The interception criteria include file types that must at least include text, images, and audio/video.

6.1.3 Intrusion Prevention

6.1.3.1 Intrusion Detection The product should be able to detect intrusion activities on the network, and at least support the detection of the following intrusion activities.

a) Trojan backdoors, denial-of-service attacks, buffer overflows, etc.;

b) SQL injection attacks, XSS attacks, third-party component vulnerability attacks, etc.

6.1.3.2 Intrusion Blocking The product should support intelligent analysis and interception of detected intrusions to prevent them from entering the target network.

6.1.3.3 Custom Features The product should allow authorized administrators to customize event characteristics, and packets that match the customized characteristics can be blocked.

6.1.3.4 Attack Evasion Recognition The product should be able to detect behaviors that evade or deceive detection, and should at least support. IP fragment reassembly, TCP stream reassembly, protocol port relocation, and URL resizing. String manipulation and shell code manipulation.

6.1.4 Malicious Program Prevention

6.1.4.1 Transmission Detection The product should have the ability to detect malicious programs transmitted via protocols such as FTP, HTTP, POP3, IMAP, and SMTP.

6.1.4.2 Transmission Blocking The product should have the ability to block malicious programs transmitted via protocols such as FTP, HTTP, POP3, IMAP, and SMTP.

6.1.4.3 Compressed File Detection The product should have the ability to detect malicious programs in compressed files and should at least support ZIP and RAR compression formats.

6.1.5 Secure Networking

6.1.5.1 Network Address Translation The product should have SNAT and DNAT functions.

6.1.5.2 Routing 6.1.5.2.1 Static Routing The product should have static routing functionality and be able to configure static routes. 6.1.5.2.2 Dynamic Routing The product should have dynamic routing capabilities, including one or more dynamic routing protocols such as RIP, OSPF, and BGP. 6.1.5.2.3 Policy Routing Products with multiple network interfaces of the same attributes (multiple external, internal, or DMZ network interfaces) should support policy routing functionality. Please provide the following.

a) Policy-based routing based on source and destination IP addresses;

b) Interface-based policy routing;

c) Policy-based routing based on protocol and port;

d) Policy-based routing based on application type;

e) Automatically select routes based on multi-link load conditions.

6.1.5.3 Virtual Private Network The product should have VPN functionality, with the following requirements.

a) The cryptographic techniques used in the configuration of the Virtual Private Network comply with the relevant requirements of GB/T 36968-2018;

b) Supports basic IKE rule configuration, such as. IKE name, type, address, protocol, authentication method, etc.;

c) Supports basic tunnel configuration, such as tunnel name, address, VPN rules, etc.

d) Supports real-time monitoring and querying of the status of established VPN tunnels, such as. name, type, local information, peer information, and traffic status. State, etc.

6.1.6 Safety Management

6.1.6.1 Unified Security Policy Configuration The product should have the ability to configure security policies uniformly for multiple threats, as required below.

a) Supports unified interface and processes for various security measures such as access control, intrusion prevention, malware prevention, and anti-spam. It provides centralized configuration and management functions, enabling the coordinated use of multiple threat protection capabilities;

b) Provide matching conditions for unified security policies, detection and analysis of contradictory or redundant policies, and effective enforcement measures;

c) Provide unified security policy management functions, including querying, creating, modifying, deleting, starting and stopping, etc.

6.1.6.2 Incident Monitoring and Handling The product should have the function of unified monitoring and handling of various security incidents, with the following requirements.

a) Supports monitoring of abnormal traffic events by source IP address, destination IP address, port, time, or protocol, or a combination thereof;

b) Supports unified monitoring of security incidents such as intrusion attempts, malware, and spam;

c) Supports unified correlation and analysis of various security events such as abnormal traffic, unauthorized access, intrusion behavior, malware, and spam. analytical ability;

d) Supports coordinated handling of multiple security incidents, including abnormal traffic, unauthorized access, intrusion attempts, malware, and spam. ability.

6.1.6.3 Security Alarms The product should have a safety alarm function, with the following requirements.

a) Issue security alerts when intrusion attempts, malware, spam, or other security incidents are detected;

b) Supports one or more security alert methods such as email, SMS, pop-up, sound, and SNMPTrap.

6.1.6.4 Management Control 6.1.6.4.1 Local Management The product should support configuration management via local CLI or a graphical management interface. 6.1.6.4.2 Remote Management The product should support secure remote management, such as remote management based on SSH or HTTPS protocols. 6.1.6.4.3 Product Upgrade The product should have upgrade functionality, with the following requirements.

a) Supports online or offline upgrades of system versions and various security capability signature libraries;

6.1.7 Security Audit