

ICS 35.240
CCS A 90

GA

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

GA/T 1714-2020

**Information security technology - Security technology
requirements for flow anomaly detection and cleaning products**

信息安全技术 异常流量检测和清洗产品安全技术要求

(English Translation)

Issued on: March 6, 2020

Implemented on: May 1, 2020

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
5 Abnormal flow detection and cleaning product description
6 General description of abnormal flow detection and cleaning products
6.1 Classification of safety technical requirements
6.2 Security classification
7 Safety function requirements
7.1 Flow Collection
7.2 SNMP monitoring
7.3 BGP route monitoring
7.4 Abnormal traffic identification
7.5 Two-way flow detection
7.6 Custom Attack Type
7.7 Abnormal traffic alarm
7.8 Alarm mode
7.9 Abnormal Traffic Handling
7.10 Equipment's own state monitoring
7.11 Management control capability
7.12 Report function
7.13 Data Security
8 Self-safety function requirements
8.1 Identification and identification
8.2 Audit function
9 Security requirements
9.1 Development
9.2 Guidance documents
9.3 Life Cycle Support
9.4 Test
9.5 Vulnerability assessment

10 Requirements for different security levels

10.1 Safety function requirements

10.2 Self-safety function requirements

10.3 Safety assurance requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009:

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security:

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security:

Drafting organizations of this standard: Computer Information System Safety Product Quality Supervision and Inspection Center of Ministry of Public Security, Third Research Institute of Ministry of Public Security, Beijing Tian Rongxin Network Security Technology Co., Ltd., Beijing China NSFOCUS Technology Co., Ltd:

1 Scope

This standard specifies the safety function requirements of abnormal flow detection and cleaning products, their own safety function requirements and safety guarantee requirements, etc:

Classification requirements:

This standard applies to the design, development and testing of abnormal flow detection and cleaning products:

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:

GB/T 18336.3-2015 Information Technology Security Technology Information Technology Security Assessment Criteria Part 3: Security Assurance Components GB/T 25069-2010 Information Security Technical Terms

3 Terms and definitions

The following terms and definitions defined in GB/T 18336.3-2015 and GB/T 25069-2010 apply to this document:

Deepflowinspection

The network device summarizes the network traffic and generates protocol packets such as NetFlow and sFlow, and analyzes the traffic characteristics through matching to determine an identification technology of abnormal traffic based on traffic statistics:

Flowcleaning

Block abnormal traffic by cutting connections, ACL filtering, static empty route filtering, etc., and inject normal traffic back to the network behavior:

4 Abbreviations

The following abbreviations apply to this document:

ACL: Access Control List (AccessControlList) BGP: Border Gateway Protocol (BorderGatewayProtocol) CC: Challenge Black Hole (ChallengeColapsar) DNS: Domain Name System (DomainNameSystem) DOS: Denial of Service (DenialofService) DDOS: Distributed Denial of Service (DistributedDenialofService) GRE: Generic Routing Encapsulation (GenericRoutingEncapsulation) HTTP: HyperText Transfer Protocol (HyperTextTransferProtocol) ICMP: Internet Control Message Protocol (InternetControlMessageProtocol)