

ICS 35.240
CCS A 90

GA

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

GA/T 403.1-2002

Replacing GA/T 403.1-2002

**Information security technology. Security technical
requirements for intrusion detection products. Part 1:
Network-based products
(English Translation)**

Issued on: January 1, 1970

Implemented on: January 1, 1970

Issued by: Ministry of Public Security

Table of Contents

Introduction	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Network Intrusion Detection Product Description	
6 Security Environment	
6.1 Hypothesis	
6.2 Threat	
4 6.3 Organization for Security Policy	
7 Security purposes	
7.1 Product Safety Objective	
7.2 Environmental security objectives	
Security functional requirements 8	
8.1 Data acquisition capabilities in claim	
8.2 Intrusion analysis Claim	
8.3 Intrusion Response 6 Functional requirements	
8.4 Management Control functional requirements	
8.5 7 processing requirements of the test results	
8.6 Product flexibility requirements	
8.7 Identification	
8.8 Management 9 Administrator	
8.9 Security Audit	
8.10 Event Data Security	
8.11 Communication Security	
8.12 Security 10 product itself	
9 Security assurance requirements	
9.1 Configuration Management	
9.2 Delivery and Operation	
12 9.3 Development	
9.4 Guidance document	

14 9.5 Life Cycle Support

9.6 Test

9.7 Vulnerability assessment

10 Basic principles of technical requirements

10.1 16 basic principles of security functional requirements

10.2 18 basic principles of security assurance requirements

11 Classification requirements

11.1 Overview

11.2 Classification of security functional requirements

11.3 Classification of security assurance requirements

Foreword

GA/T 403 "information security technology intrusion detection product safety technical requirements" is divided into two parts.

--- Part 1. network products;

--- Part 2. Host products.

This section GA/T Part 1 403.

This section drafted in accordance with GB/T 1.1-2009 given rules.

This Part replaces GA/T 403.1-2002 "IT intrusion detection products safety - Part 1. network products", Compared with GA/T 403.1-2002 main technical changes are as follows.

--- Standard name was changed to "information security technology intrusion detection products - Safety requirements - Part 1. Network products";

--- Increased network intrusion detection product description (see Chapter 5);

--- Increase the security environment, including the assumptions, threats and organizational security policies (see Chapter 6);

--- Increased security purposes, including the purpose of product safety and environmental safety purposes (see Chapter 7);

--- Remove the network intrusion detection product performance requirements (see the 2002 edition, Chapter 7);

--- Deleted the database support (see the 2002 edition of 6.1.5.5);

--- Modify the content of security functional requirements (see Chapter 8, Chapter 8, 2002

edition);

--- Increase the technical requirements of the basic principles, including the basic principles of security functional requirements and security assurance requirements for the basic principles (see Chapter 10).

Please note that some of the content of this document may involve patents. Release mechanism of the present document does not assume responsibility for the identification of these patents.

This part is proposed by the Ministry of Public Security Network Security Protection Agency.

This part of the jurisdiction of the Ministry of Public Security Information System Standardization Technical Committee.

This section drafted by. Ministry of Public Security of Computer Information System Security Product Quality Supervision and Inspection Center, Blue Shield Information Security Technology Co. Shares Companies, Third Institute of Ministry of Public Security.

Introduction

GA/T 403 is described in detail in this section of the network-based intrusion detection products and security environment related assumptions, threats and organizational security policies Strategy, defines the purpose of network security intrusion detection products and their supporting environment, demonstrated by the basic principles of security functional requirements and can be traced back Products covered security purposes, for security purposes can be traced back cover and secure environment-related assumptions, threats and organizational security policies.

This section basically level with reference to the GB/T 18336.3-2008 prescribed level EAL2 security assurance requirements, and enhance the level at EAL4 level Security assurance requirements based on the vulnerability analysis requires upgrade to an attacker can withstand moderate attack potential attack.

This section only gives a network-based intrusion detection products should meet the technical requirements of safety, but network-based intrusion detection products of specific skills Art implementations, a method is not required.

Information Security Technology Intrusion detection products safety technical requirements Part 1. Network products

1 Scope

GA/T 403 provisions of this part of the network-based intrusion detection products, security functional requirements, security assurance requirements and grading requirements.

This section applies to the design, development and testing network-based intrusion detection products.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB 17859-1999 computer information system security protection classification criterion
GB/T 18336-2008 (all parts), Information technology - Security techniques - Information Technology Security Evaluation Guidelines GB/T 25069-2010 Information security technology terms

3 Terms and Definitions

GB 17859-1999, GB/T 18336-2008 (all parts) and GB/T 25069-2010 defined and the following terms and definitions Meaning applicable to this document.

Intrusion

Any attempt to harm the integrity of resources, confidentiality or availability of behavior.

Detector sensor

Collection may indicate intrusions or misuse of information system resources in real-time event, and the information collected for preliminary points Analysis of network-based intrusion detection product components. Installed at key nodes in the network, and monitor data flowing through the network.

Console managementconsole Detector for management, policy configuration, data management, alarm management, incident response, as well as other event repository upgrade management, and the Invasion behavior of intrusion detection system components in-depth analysis. A console can manage multiple detectors.

Attack signatures attacksignature Intrusion detection systems pre-defined information can be found in a specific attack is happening.

Alarms alert

When the attack or invasion, intrusion detection system, emergency notification issued to the authorized administrator.