ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1714—2020

信息安全技术
异常流量检测和清洗产品安全技术要求

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

2020-03-06 发布　　2020-05-01 实施

中华人民共和国公安部　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司。

本标准主要起草人：胡亚兰、冯婷婷、刘继顺、俞优、李毅、赵婷、雷晓锋、叶晓虎。

信息安全技术
异常流量检测和清洗产品安全技术要求

1 范围

本标准规定了异常流量检测和清洗产品的安全功能要求、自身安全功能要求和安全保障要求及等级划分要求。

本标准适用于异常流量检测和清洗产品的设计、开发与测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

深度流检测 deep flow inspection

网络设备将网络流量汇总并生成 NetFlow 和 sFlow 等协议报文，并通过匹配分析流量特征，判断异常流量的一种基于流量统计特征的识别技术。

3.2

流量清洗 flow cleaning

通过切断连接、ACL 过滤、静态空路由过滤等方式阻断异常流量，并将正常流量回注到网络中的行为。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表(Access Control List)

BGP：边界网关协议(Border Gateway Protocol)

CC：挑战黑洞(Challenge Collapsar)

DNS：域名系统(Domain Name System)

DOS：拒绝服务(Denial of Service)

DDOS：分布式拒绝服务(Distributed Denial of Service)

GRE：通用路由封装协议(Generic Routing Encapsulation)

HTTP：超文本传送协议(Hyper Text Transfer Protocol)

ICMP：网际控制报文协议(Internet Control Message Protocol)