ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1177—2014

信息安全技术
第二代防火墙安全技术要求

Information security technology—Security technique requirements for the second generation firewall products

2014-07-24 发布　　2014-09-01 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提出并归口。

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、深圳市深信服电子科技有限公司、网神信息技术(北京)股份有限公司、北京神州绿盟信息安全科技股份有限公司、网御星云信息技术有限公司、启明星辰信息技术有限公司。

本标准主要起草人：邹春明、俞优、宋好好、陆臻、顾健、李焕波、王帆、王刚、段继平、冯涛、黄涛。

信息安全技术
第二代防火墙安全技术要求

1 范围

本标准规定了第二代防火墙产品的安全功能要求、安全保证要求、环境适应性要求、性能要求和安全等级划分。

本标准适用于第二代防火墙产品的设计、开发和测试。

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 17859—1999 计算机信息系统安全保护划分准则

GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求

GB/T 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 20281—2006 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

第一代防火墙 firewall

一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统，具备包过滤、网络地址转换(NAT)、状态检测等安全功能。

3.2

第二代防火墙 the second generation firewall

除具备第一代防火墙基本功能之外，还具有应用流量识别、应用层访问控制、应用层安全防护、用户控制、深度内容检测、高性能等特征的控制的系统。

3.3

深度内容检测 deep content inspection

对应用协议进行深入解析，识别出协议中的各种要素(如，针对 http 协议，可具体解析到如 cookie、Get 参数、Post 表单等内容)及协议所承载的业务内容(如，业务系统交互中包含在协议或文件中的数据内容)，并对这些数据进行快速解析，以还原其原始通信的信息。根据解析后的原始信息，检测其中是否包含威胁以及敏感内容。

3.4

SQL 注入 SQL injection

把 SQL 命令插入到 web 表单递交或者页面请求的参数中，以达到欺骗服务器执行恶意 SQL 命令的目的。