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

GA/T 1177—2014

中华人民共和国公共安全
行　业　标　准
信息安全技术
第二代防火墙安全技术要求
GA/T 1177—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323　发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.5　字数 33 千字
2014年10月第一版　2014年10月第一次印刷
*
书号:155066·2-27378　定价 24.00 元

GA/T 1177-2014

5.4.2.5 支持能力

第二代防火墙应至少支持以下一种 IPv6 过渡网络环境：

a） 双协议栈：IPv4/IPv6 双栈网络环境，能够在 IPv4/IPv6 双栈网络环境下正常工作；

b） 协议转换：将 IPv4 和 IPv6 两种协议相互转换，能够在协议转换网络环境下正常工作；

c） 隧道：至少支持以下一种隧道工作模式：

1） 6over4 网络环境，能够在 6over4 网络环境下正常工作；

2） ISATAP 网络环境，保证在 ISATAP 网络环境下正常工作。

5.5 性能要求

5.5.1 应用层吞吐量

流量参考场景构成如下：HTTP Text，20%；HTTP Audio，4%；HTTP Video 5%，SMB，8%；SMTP，12%；POP3，12%；FTP，10%；SSH，2%；TELNET，2%；PostgreSQL 5%；其他，20%。

应用层吞吐量视不同速率的第二代防火墙有所不同，具体指标要求如下：

a） 第二代防火墙在不阻断正常连接的情况下，应达到的单向应用层吞吐量指标：

1） 千兆第二代防火墙应用层吞吐量应不小于 900 Mbps；

2） 万兆第二代及万兆以上防火墙应用层吞吐量应不小于 8 Gbps；

b） 开启入侵防御、恶意代码防御及应用识别功能的情况下，按照上述流量场景，防火墙不能误拦截正常的 TCP 连接，第二代防火墙应用层吞吐量下降不超过原来的 30%。

5.5.2 网络层吞吐量

网络层吞吐量视不同速率的第二代防火墙有所不同，具体指标要求如下：

a） 第二代防火墙在不丢包的情况下，一对相应速率的端口在具有多条(200 条)包过滤规则的条件下应达到的双向吞吐量指标：

1） 对 64 字节短包，千兆第二代防火墙应不小于线速的 50%，万兆第二代防火墙应不小于线速的 70%；

2） 对 512 字节中长包，千兆第二代防火墙应不小于线速的 85%，万兆第二代防火墙应不小于线速的 90%；

3） 对 1 518 字节长包，千兆第二代防火墙应不小于线速的 95%，万兆第二代防火墙应不小于线速的 98%；

b） 在开启入侵防御、恶意代码防御及应用识别功能的条件下，第二代防火墙吞吐量下降不超过原来的 30%。

5.5.3 延迟

延迟视不同速率的第二代防火墙有所不同，在最大吞吐量 90%的条件下，具体延迟指标要求如下：

a） 千兆第二代防火墙的 64 字节短包平均延迟不应超过 500 μs；

b） 万兆第二代防火墙的 64 字节短包平均延迟不应超过 90 μs；

c） 在开启入侵防御、恶意代码防御及应用识别功能的条件下，第二代防火墙平均延迟增加应不超过原来的 50%。

5.5.4 最大新建连接速率

最大新建连接速率视不同速率的第二代防火墙有所不同，具体指标要求如下：

目　次

5.3.6.2 测试：高层设计

开发者应提供测试深度的分析。

深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

5.3.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，应表明测试成功后的预期输出；

d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

5.3.6.4 独立测试

5.3.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.3.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

5.3.7 脆弱性评定

5.3.7.1 误用

5.3.7.1.1 指南审查

开发者应提供指导性文档，指导性文档应满足以下要求：

a) 标识所有可能的产品运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义；

b) 完备的、清晰的、一致的、合理；

c) 列出关于预期使用环境的所有假设；

d) 列出对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

5.3.7.1.2 分析确认

开发者应提供完备的分析文档论证指导性文档。

5.3.7.2 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

5.3.7.3 脆弱性分析

5.3.7.3.1 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

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。