ICS 35.040
L 80

GA

中华人民共和国公共安全行业标准

GA/T 1539—2018

信息安全技术
网络病毒监控系统
安全技术要求和测试评价方法

Information security technology Security technical requirements and evaluation approaches for virus detection system products

2018－12－27 发布　　2018－12－27 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：国家计算机病毒应急处理中心、公安部十一局七处、信息产业信息安全测评中心、国家信息中心、天津市公安局网络安全保卫总队、北京工业大学、北京瑞星信息技术有限公司、北京安天网络安全技术有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新（北京）科技股份公司、北京神州绿盟信息安全科技股份有限公司、北京天融信科技有限公司。

本标准主要起草人：陈建民、杜振华、张俊兵、陆磊、曹鹏、张喆、张瑞、刘彦、黄一斌、李冬、孟彬、张鑫、刘健、禄凯、王冠、王世玉、叶荣军、赵焕菊、杨绍波、徐雨晴、崔婷婷、焦玉峰、王龑。

信息安全技术 网络病毒监控系统安全技术要求和测试评价方法

1 范围

本标准规定了网络病毒监控系统的功能要求、安全要求、性能要求及安全保障要求，并给出了测试评价方法。

本标准适用于网络病毒监控系统的设计、开发及检测。

2 术语和定义

下列术语和定义适用于本文件。

2.1

网络病毒监控系统 virus detection system

旁路方式监听网络内的数据包并进行分析，以发现网络中传播的病毒及其相关行为的系统。

2.2

病毒 virus

能够影响计算机操作系统、应用程序和数据的完整性、可用性、可控性和保密性的计算机程序或代码，包括文件型病毒、蠕虫、木马程序、宏病毒、脚本病毒等恶意程序。

2.3

病毒捕获 virus capture

网络病毒监控系统为保留病毒或疑似病毒样本以及受感染的文件，而将从网络上捕获的相应文件存储在特定的受限制存储空间的处理方式。

2.4

内部网络 internal network

通过防火墙/网络病毒监控系统隔离的可信任区域或保护区域。

2.5

外部网络 external network

通过防火墙/网络病毒监控系统隔离的不可信任区域或非保护区域。

2.6

线速 wire speed

网络病毒监控系统所监控网络环境理论上能达到的最大转发速率。

2.7

负载量 peak load

网络病毒监控系统在不丢包的情况下处理监控数据的能力，一般以能达到的线速（或称通过速率）的百分比来表示。

2.8

恶意URL malicious URL

指向的资源中含有病毒的URL。

2.9

加壳病毒 packed virus

通过特定算法的变换，将病毒的编码进行一次或多次的压缩、加密，产生新的病毒文件。与原病毒文件相比，文件内容发生变化，但功能保持不变。

2.10

可执行病毒样本 executable virus sample

可以被激活并正常执行其功能的病毒样本文件。

2.11

恶意网页脚本样本 malicious webpage script virus sample

含有漏洞利用、后门、远程控制等恶意代码的恶意网页或脚本病毒样本文件。

2.12

已知病毒样本 known virus sample

网络病毒监控系统能够检测的病毒样本文件。

2.13

病毒样本库 virus sample set

病毒样本文件的集合。

3 缩略语

下列缩略语适用于本文件。

URL：统一资源定位符（Uniform Resource Locator）
IP：互联网协议（Internet Protocol）
TCP：传输控制协议（Transmission Control Protocol）
HTTP：超文本传输协议（HyperText Transfer Protocol）
SMB：服务器消息块协议（Server Message Block）
CIFS：通用网络文件系统协议（Common Internet File System）
IPv4：互联网协议第4版（Internet Protocol Version 4）
IPv6：互联网协议第6版（Internet Protocol Version 6）
FTP：文件传输协议（File Transfer Protocol）
POP3：邮局协议第3版（Post Office Protocol version 3）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
IMAP：Internet邮件访问协议（Internet Mail Access Protocol）
HTML：超文本标记语言（HyperText Markup Language）
XLS：微软公司电子表格文档格式（Microsoft Excel）
CSV：逗号分隔的文本文件格式（Comma-Separated Values）
XML：可扩展标记语言（Extensible Markup Language）
Gbps：千兆/秒（Gigabits Per Second）
KB：千字节（Kilo Byte）
HTTPS：安全超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer）
IDS：入侵检测系统（Intrustion Detection System）
IPS：入侵防御系统（Intrustion Prevention System）

4 网络病毒监控系统描述

网络病毒监控系统以旁路方式接入网络，能够实时监测网络环境中的病毒疫情发展趋势；全面检测各种网络病毒的扫描、传输、攻击等行为；精确定位病毒的来源；评估病毒产生的网络压力状况；并准确提供病毒类别、病毒名称等信息；形成网络病毒的全局视图。

这种网络病毒监控系统能够检测网络内部的数据，对多种网络协议和应用协议的数据进行分析和病毒扫描，一旦发现病毒就会采取告警，并定位病毒文件及其来源、病毒类别、病毒名称等信息，实现病毒大规模爆发前的预警。一些网络病毒监控系统还可以与其它安全设备进行交互，对病毒传播行为进行阻断。

网络病毒监控系统运行环境和工作模式参见附录A中A.1和A.2。

5 技术要求

5.1 总体说明

5.1.1 技术要求分类

将网络病毒监控系统安全技术要求分为功能、安全、性能和安全保障要求四个大类。其中，功能要求是对网络病毒监控系统应具备的功能提出具体的要求，包括安全监测能力、监控策略、响应处理、报表和统计、加密应用协议支持、故障信息告警、升级能力、协同能力等；性能要求是对网络病毒监控系统应达到的性能指标做出规定，例如负载量；安全要求是对网络病毒监控系统自身安全和防护能力提出具体的要求，例如标识与鉴别、安全管理、审计日志等；安全保障要求则针对网络病毒监控系统开发者和网络病毒监控系统自身提出具体的要求，例如开发、指导性文档、生命周期支持、测试、脆弱性评定等。

5.1.2 安全等级

根据国内测评认证机构、测评技术和我国网络病毒监控系统产品开发现状，对网络病毒监控系统产品进行安全等级划分。安全等级分为基本级和增强级。安全等级划分标准主要依据产品的功能特性，对基本级产品的性能不作要求。

增强级产品除需满足基本级产品的技术要求外，还需满足增强级中列出的其他技术要求。其中“**加粗宋体字**”表示所描述的要求仅适用于增强级产品。

5.2 功能要求

5.2.1 基本级

5.2.1.1 监测能力

5.2.1.1.1 数据收集

网络病毒监控系统应具有实时获取被监控网络内的数据包和数据流的能力。获取的数据包和数据流应足以进行病毒检测和分析。

5.2.1.1.2 应用协议支持

产品应支持对使用以下应用协议的网络请求和响应进行病毒检测和分析：

a) HTTP 协议；
b) FTP 协议；
c) POP3 协议；
d) SMTP 协议；
e) SMB/CIFS 协议。

5.2.1.1.3 静态病毒检测

当处于静态非激活的病毒在被监控网络中传播时，产品应具有相应的响应处理能力，并且对于正常的系统文件和文档不会产生误报警。

5.2.1.1.4 逃避检测防护

产品应能支持识别压缩格式的病毒文件，以此发现逃避检测的病毒传播行为。

5.2.1.1.5 多种类型网络应用场景支持

为适应不同类型网络，产品应具有以下能力：

a) 产品支持在纯 IPv4/IPv6 网络应用场景中安装与正常使用；
b) 产品支持 IPv4 与 IPv6 双协议栈，可以在 IPv4 与 IPv6 共存的网络应用场景中安装与正常使用。

5.2.1.2 监控策略

5.2.1.2.1 策略自定义

产品应能根据5.2.1.1中所述的要求添加、修改和删除监控策略。

5.2.1.2.2 策略初始模板

产品应具备初始的监控策略，并覆盖5.2.1.1.2中所述的常见应用协议，并开启对病毒文件的检测功能。

5.2.1.3 响应处理

5.2.1.3.1 病毒检测

产品应能根据监控策略对病毒文件进行检测和告警。

5.2.1.3.2 告警信息

产品应能对病毒传播行为提供报警功能。报警信息应至少包括以下内容：

a) 病毒传播来源地址；
b) 病毒传播来源端口号；
c) 病毒传播目的地址；
d) 病毒传播目的端口号；
e) 病毒传播协议；
f) 病毒文件名；
g) 病毒名称；
h) 事件发生的日期和时间。

5.2.1.3.3 告警方式

产品告警应采用屏幕实时提示、邮件告警、短信告警和声音告警等一种或多种方式。

5.2.1.3.4 事件记录

产品应能对病毒传播行为及时生成事件记录，事件记录应存储于掉电非易失性存储介质中，且在存储空间达到阈值时能够通知授权管理员。

5.2.1.4 报表和统计

5.2.1.4.1 报表生成

产品应能对事件记录进行统计，并根据以下模板生成报表：

a) 缺省报表模板；
b) 自定义报表模板。

5.2.1.4.2 报表导出

产品报表应能输出成方便阅读的文件格式，至少支持以下报表文件格式中的一种或多种：DOC、PDF、HTML、XLS、CSV、XML等。

5.2.1.4.3 统计功能

产品应提供基于时间、主机地址、威胁事件类型等进行统计的功能。

5.2.1.5 故障信息告警

产品应具备软、硬件故障告警功能，能够在软件、硬件出现故障时，通过屏幕实时提示、邮件告警、短信告警、声音告警等一种或多种方式进行告警。

5.2.1.6 升级能力

产品应支持手动或自动的方式进行升级，对病毒库、策略文件以及服务程序等进行更新。

5.2.2 增强级

5.2.2.1 监测能力

5.2.2.1.1 数据收集

网络病毒监控系统应具有实时获取被监控网络内的数据包和数据流的能力。获取的数据包和数据流

应足以进行病毒检测和分析。

5.2.2.1.2 应用协议支持

产品应支持对使用以下应用协议的网络请求和响应进行病毒检测和分析：

a) HTTP 协议；
b) FTP 协议；
c) POP3 协议；
d) SMTP 协议；
e) SMB/CIFS 协议；
f) 其它协议。

5.2.2.1.3 静态病毒检测

当处于静态非激活的病毒在被监控网络中传播时，产品应具有相应的响应处理能力，并且对于正常的系统文件和文档不会产生误报警。

5.2.2.1.4 动态病毒检测

当处于动态已激活的病毒在被监控网络中传播时，产品应具有相应的响应处理能力。

5.2.2.1.5 逃避检测防护

产品应能支持识别以下特殊格式的病毒文件，以此发现逃避检测的病毒传播行为：

a) 压缩格式的病毒文件；
b) 加壳格式的病毒文件。

5.2.2.1.6 恶意 URL 防护

对于含有病毒、木马等恶意软件的恶意 URL，产品应具有相应的响应处理能力。

5.2.2.1.7 多种类型网络应用场景支持

为适应不同类型网络，产品应具有以下能力：

a) 产品支持在纯 IPv4/IPv6 网络应用场景中安装与正常使用；
b) 产品支持 IPv4 与 IPv6 双协议栈,可以在 IPv4 与 IPv6 共存的网络应用场景中安装与正常使用。

5.2.2.2 监控策略

5.2.2.2.1 策略自定义

产品应能根据5.2.2.1中所述的要求添加、修改和删除监控策略。

5.2.2.2.2 策略初始模板

产品应具备初始的监控策略，并覆盖5.2.2.1.2中所述的常见应用协议，并开启对病毒文件的检测功能。

5.2.2.3 响应处理

5.2.2.3.1 病毒检测

产品应能根据监控策略对病毒文件进行检测和告警。

5.2.2.3.2 病毒捕获

产品应能根据监控策略对病毒文件进行捕获。

5.2.2.3.3 恶意 URL 检测

产品应能根据防护策略对恶意 URL 的访问请求进行检测与告警。

5.2.2.3.4 告警信息

产品应能对病毒传播行为提供报警功能。报警信息应至少包括以下内容：

a) 病毒告警信息：
   1) 病毒传播来源地址；
   2) 病毒传播来源端口号；
   3) 病毒传播目的地址；
   4) 病毒传播目的端口号
   5) 病毒传播协议；
   6) 病毒文件名；
   7) 病毒名称；
   8) 事件发生的日期和时间；

b) 恶意 URL 告警信息：
   1) 恶意 URL 地址；
   2) 访问恶意 URL 地址的 IP 地址；
   3) 恶意 URL 描述；
   4) 事件发生的日期和时间。

5.2.2.3.5 告警方式

产品告警应采用屏幕实时提示、邮件告警、短信告警和声音告警等一种或多种方式。

5.2.2.3.6 事件记录

产品应能对病毒传播行为及时生成事件记录，事件记录应存储于掉电非易失性存储介质中，且在存储空间达到阈值时能够通知授权管理员。

5.2.2.4 报表和统计

5.2.2.4.1 报表生成

产品应能对事件记录进行统计，并根据以下模板生成报表：

a) 缺省报表模板；
b) 自定义报表模板。

5.2.2.4.2 报表导出

产品报表应能输出成方便阅读的文件格式，至少支持以下报表文件格式中的一种或多种：DOC、PDF、HTML、XLS、CSV、XML等。

5.2.2.4.3 统计功能

产品应提供基于时间、主机地址、威胁事件类型等进行统计的功能。

5.2.2.5 异常流量处理

产品应对于以下几种异常流量进行有效的处理：

a) 碎片包；

b) 畸形报文；

c) 其他异常流量。

5.2.2.6 故障信息告警

产品应具备软、硬件故障告警功能，能够在软件、硬件出现故障时，通过屏幕实时提示、邮件告警、短信告警、声音告警等一种或多种方式进行告警。

5.2.2.7 升级能力

产品应支持手动或自动的方式进行升级：

a) 对病毒库、策略文件以及服务程序等进行更新；

b) 支持增量升级。

5.2.2.8 协同联动能力

产品应支持与其他安全产品的协同联动功能（例如与防病毒网关、防火墙等），具体要求如下：

a) 网络病毒监控系统按照一定的安全协议与其他安全产品协同联动，并支持手动与自动方式来配置联动策略；

b) 网络病毒监控系统在协同联动前与其联动的安全产品进行身份鉴别。

5.3 安全要求

5.3.1 基本级

5.3.1.1 标识与鉴别

5.3.1.1.1 管理员标识

5.3.1.1.1.1 属性定义

产品应为每个管理员规定与之相关的安全属性，如标识、鉴别信息、隶属组、权限等。

5.3.1.1.1.2 属性初始化

产品应提供使用默认值对创建的每个授权管理员的属性进行初始化的能力。

5.3.1.1.1.3 唯一性标识

产品应为授权管理员提供唯一标识，并能将标识与该授权管理员的所有可审计事件相关联。

5.3.1.1.2 身份鉴别

5.3.1.1.2.1 基本鉴别

产品应在执行任何与安全功能相关的操作之前采用一种身份鉴别方式鉴别授权管理员的身份。

5.3.1.1.2.2 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

5.3.1.2 安全管理

5.3.1.2.1 安全功能管理

授权管理员应能对产品进行以下管理操作：

a) 查看、修改相关安全属性；
b) 启动、关闭全部或部分安全功能；
c) 制定和修改各种安全策略。

5.3.1.2.2 安全管理方式

产品应向授权管理员提供以下安全管理方式：

a) 通过 console 进行本地管理；
b) 通过网络接口进行远程管理。

5.3.1.3 审计日志

5.3.1.3.1 审计日志生成

产品应对与自身安全相关的以下事件生成审计日志：

a) 授权管理员登录成功和失败；
b) 对安全策略进行更改；
c) 对授权管理员进行增加、删除和属性修改；
d) 因鉴别失败的次数超出了设定值，导致的会话连接终止；
e) 对事件记录、审计日志的操作；
f) 授权管理员的其他操作。

每一条审计日志至少应包括事件发生的日期、时间、管理员标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

5.3.1.3.2 审计日志存储

审计日志应存储于掉电非易失性存储介质中，且默认最低保存期限不少于六个月。

5.3.1.3.3 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权管理员访问审计日志；
b) 提供对审计日志的查询功能；
c) 保存并导出审计日志。

5.3.2 增强级

5.3.2.1 标识与鉴别

5.3.2.1.1 管理员标识

5.3.2.1.1.1 属性定义

产品应为每个授权管理员规定与之相关的安全属性，如标识、鉴别信息、隶属组、权限等。

5.3.2.1.1.2 属性初始化

产品应提供使用默认值对创建的每个授权管理员的属性进行初始化的能力。

5.3.2.1.1.3 唯一性标识

产品应为授权管理员提供唯一标识，并能将标识与该授权管理员的所有可审计事件相关联。

5.3.2.1.2 身份鉴别

5.3.2.1.2.1 基本鉴别

产品在执行任何与安全功能相关的操作之前鉴别授权管理员的身份：

a) 产品应采用一种授权管理员身份鉴别方式；

b) 产品应对同一授权管理员采用两种或两种以上组合的用户身份鉴别方式。

5.3.2.1.2.2 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

5.3.2.1.3 鉴别失败处理

当对授权管理员鉴别失败的次数达到指定次数后，产品应能终止授权管理员的访问。

5.3.2.2 安全管理

5.3.2.2.1 安全功能管理

授权管理员应能对产品进行以下管理操作：

a) 查看、修改相关安全属性；

b) 启动、关闭全部或部分安全功能；

c) 制定和修改各种安全策略。

5.3.2.2.2 安全角色权限分离

产品能够对特权角色和权限进行区分：

a) 产品应具有至少两种不同权限的安全角色，如：管理员和审计员；

b) 产品应对特权角色采用最小授权原则，如：管理员不能对审计员负责的审计功能进行管理，审计员也不能对管理员负责的功能进行管理。

5.3.2.2.3 安全管理方式

产品应向授权管理员提供以下安全管理方式：

a) 通过 console 进行本地管理；

b) 通过网络接口进行远程管理；

c) 采取保密措施保障远程管理的信息传输安全。

5.3.2.2.4 远程保密传输

若产品组件间通过网络进行通讯，应采取保密措施保障组件间数据传输的安全。

5.3.2.2.5 远程管理主机

若控制台提供远程管理功能，应能对可远程管理的主机地址进行限制。

5.3.2.2.6 数据完整性

产品应确保授权管理员信息、策略信息和关键程序的数据完整性，应采取必要的手段对其完整性自动进行检验。

5.3.2.2.7 安全支撑系统

产品的底层支撑系统应满足以下要求：

a) 确保其支撑系统不提供多余的网络服务；

b) 不含任何导致产品权限丢失、拒绝服务等已知的安全漏洞。

5.3.2.3 审计日志

5.3.2.3.1 审计日志生成

产品应对与自身安全相关的以下事件生成审计日志：

a) 授权管理员登录成功和失败；

b) 对安全策略进行更改；

c) 对授权管理员进行增加、删除和属性修改；

d) 因鉴别失败的次数超出了设定值，导致的会话连接终止；

e) 对事件记录、审计日志的操作；

f) 授权管理员的其他操作。

每一条审计日志至少应包括事件发生的日期、时间、管理员标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

5.3.2.3.2 审计日志存储

审计日志应存储于掉电非易失性存储介质中，且默认最低保存期限不少于六个月。

5.3.2.3.3 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权管理员访问审计日志；

b) 提供对审计日志的查询功能；

c) 保存并导出审计日志。

5.4 安全保障要求

5.4.1 基本级

5.4.1.1 开发

5.4.1.1.1 安全架构描述

开发者应向评估者提供产品安全功能安全架构的描述，安全架构的描述应满足以下要求：

a) 与在产品设计文档中对安全功能要求执行的抽象描述的级别一致；

b) 描述与安全功能要求一致的产品安全功能安全域；

c) 描述产品安全功能初始化过程为何是安全的；

d) 安全架构的描述论证产品安全功能可防止被破坏；

e) 安全架构的描述论证产品安全功能可防止安全功能要求执行的功能被旁路。

5.4.1.1.2 安全执行功能规范

开发者应向评估者提供一个功能规范，功能规范应满足以下要求：

a) 完整地描述产品安全功能；
b) 描述所有的产品安全功能接口的目的、使用方法以及每个安全功能接口相关的所有参数；
c) 对于每个安全功能要求，功能规范描述执行安全功能接口相关的安全功能执行行为；
d) 对于安全功能要求，功能规范描述由安全功能执行行为相关处理而引起的直接错误信息；
e) 功能规范论证安全功能要求到安全功能接口的对应关系。

5.4.1.1.3 基础设计

开发者应向评估者提供产品的设计文档，并提供从功能规范的产品安全功能接口到产品设计中获取到的最低层分解的映射，应满足以下要求：

a) 设计文档根据子系统描述产品的结构；
b) 设计文档标识产品安全功能的所有子系统；
c) 设计文档对每一个安全功能要求支撑或安全功能要求无关的产品安全功能子系统的行为进行足够详细的描述，以确定它不是安全功能要求执行；
d) 设计文档概括安全功能要求执行子系统的安全功能要求执行行为；
e) 设计文档描述产品安全功能的安全功能要求执行子系统间的相互作用，以及产品安全功能的安全功能要求执行子系统与其它产品安全功能子系统间的相互作用；
f) 映射关系证明产品设计中描述的所有行为能够映射到调用它的产品安全功能接口。

5.4.1.2 指导性文档

5.4.1.2.1 准备程序

开发者应向评估者提供产品的准备程序，满足以下要求：

a) 准备程序描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 准备程序描述安全安装产品以及安全准备与安全目标中描述的运行环境安全目的一致的运行环境必需的所有步骤。

5.4.1.2.2 操作用户指南

开发者应向评估者提供明确和合理的操作用户指南，操作用户指南应满足以下要求：

a) 操作用户指南对每一种用户角色进行描述，在安全处理环境中应被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 操作用户指南对每一种用户角色进行描述，怎样以安全的方式使用产品提供的可用接口；
c) 操作用户指南对每一种用户角色进行描述，可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 操作用户指南对每一种用户角色明确说明，与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变产品安全功能所控制实体的安全特性；
e) 操作用户指南标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），它们与维持安全运行之间的因果关系和联系；
f) 操作用户指南对每一种用户角色进行描述，为了充分实现安全目标中描述的运行环境安全目的所必须执行的安全策略。

5.4.1.3 生命周期支持

5.4.1.3.1 配置管理系统的使用

开发者应向评估者使用配置管理系统，提供配置管理文档，并满足以下要求：

a) 给产品标记唯一参照号；
b) 配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项。

5.4.1.3.2 部分产品配置管理覆盖

开发者应向评估者提供产品配置项列表，满足以下要求：

a) 配置项列表包括：产品本身、安全保障要求的评估证据和产品的组成部分；
b) 配置项列表唯一标识配置项；
c) 对于每一个产品安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

5.4.1.3.3 交付程序

开发者应将把产品或其部分交付给消费者的程序文档化，并满足以下要求：

a) 交付文档描述，在向消费者分发产品版本时，用以维护安全性所必需的所有程序；
b) 确认开发者在使用交付程序。

5.4.1.4 测试

5.4.1.4.1 覆盖证据

开发者应向评估者提供测试覆盖的证据，在测试覆盖证据中，应表明测试文档中的测试与功能规范中的安全功能接口是对应的。

5.4.1.4.2 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，标识要执行的测试并描述执行每个测试的方案，这些方案应包括对于其它测试结果的任何顺序依赖性；
b) 预期的测试结果，指出测试成功执行后的预期输出；
c) 实际的测试结果，确认和预期的测试结果的一致性。

5.4.1.4.3 独立测试—抽样

开发者应向评估者提供一组与开发者产品安全功能测试中同等的一系列资源，用于安全功能的抽样测试。

5.4.1.5 脆弱性分析

开发者应向评估者提供适合测试的产品，并提供执行脆弱性分析的相关资源，包括指导性文档、功能规范、产品设计和安全架构描述。

5.4.2 增强级

5.4.2.1 开发

5.4.2.1.1 安全架构描述

开发者应向评估者提供产品安全功能安全架构的描述，安全架构的描述应满足以下要求：

a) 与在产品设计文档中对安全功能要求执行的抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 安全架构的描述论证产品安全功能可防止被破坏；
e) 安全架构的描述论证产品安全功能可防止安全功能要求执行的功能被旁路。

5.4.2.1.2 完备的功能规范

开发者应向评估者提供一个功能规范，功能规范应满足以下要求：
a) 完整地描述产品安全功能；
b) 描述所有的产品安全功能接口的目的、使用方法以及每个安全功能接口相关的所有参数；
c) **对于每个安全功能要求，功能规范描述执行安全功能接口相关的所有行为；**
d) **功能规范描述可能由每个安全功能接口的调用而引起的所有直接错误消息；**
e) 功能规范论证安全功能要求到安全功能接口的对应关系。

5.4.2.1.3 基础模块设计

开发者应向评估者提供产品的设计文档，并提供从功能规范的产品安全功能接口到产品设计中获取到的最低层分解的映射，应满足以下要求：
a) 设计文档根据子系统描述产品的结构；
b) **设计文档根据模块描述产品安全功能；**
c) **设计文档标识产品安全功能的所有子系统，描述每一个产品安全功能子系统以及产品安全功能所有子系统间的相互作用；**
d) **设计文档提供产品安全功能子系统到产品安全功能模块间的映射关系；**
e) **设计文档描述每一个安全功能要求执行模块，包括它的目的及与其它模块间的相互作用；**
f) **设计文档描述每一个安全功能要求执行模块，包括它的安全功能要求相关接口、其它接口的返回值、与其它模块间的相互作用及调用的接口；**
g) **设计文档描述每一个安全功能要求支撑或安全功能要求无关模块，包括它的的目的及与其它模块间的相互作用；**
h) 映射关系证明产品设计中描述的所有行为能够映射到调用它的产品安全功能接口。

5.4.2.1.4 安全功能实现表示

开发者应以开发人员使用的形式提供实现表示，并向评估者提供产品设计描述与实现表示实例之间的映射，应满足以下要求：
a) **实现表示包含全部产品安全功能；**
b) **实现表示详细地定义安全功能，使得无须进一步设计就能生成安全功能；**
c) **产品设计描述与实现表示示例之间的映射能证明它们的一致性。**

5.4.2.2 指导性文档

5.4.2.2.1 准备程序

开发者应向评估者提供产品的准备程序，满足以下要求：
a) 准备程序描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 准备程序描述安全安装产品以及安全准备与安全目标中描述的运行环境安全目的一致的运行

环境必需的所有步骤。

5.4.2.2.2 操作用户指南

开发者应向评估者提供明确和合理的操作用户指南，操作用户指南应满足以下要求：

a) 操作用户指南对每一种用户角色进行描述，在安全处理环境中应被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 操作用户指南对每一种用户角色进行描述，怎样以安全的方式使用产品提供的可用接口；
c) 操作用户指南对每一种用户角色进行描述，可用功能和接口，尤其是受用户控制的所有安全参数，适当时应指明安全值；
d) 操作用户指南对每一种用户角色明确说明，与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变产品安全功能所控制实体的安全特性；
e) 操作用户指南标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），它们与维持安全运行之间的因果关系和联系；
f) 操作用户指南对每一种用户角色进行描述，为了充分实现安全目标中描述的运行环境安全目的所必须执行的安全策略。

5.4.2.3 生命周期支持

5.4.2.3.1 配置管理系统的使用

开发者应向评估者使用配置管理系统，提供配置管理文档，并满足以下要求：

a) 给产品标记唯一参照号；
b) 配置管理文档描述用于唯一标识配置项的方法；
c) 配置管理系统唯一标识所有配置项。

5.4.2.3.2 部分产品配置管理覆盖

开发者应向评估者提供产品配置项列表，满足以下要求：

a) 配置项列表包括：产品本身、安全保障要求的评估证据和产品的组成部分；
b) 配置项列表唯一标识配置项；
c) 对于每一个产品安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

5.4.2.3.3 生产支持和接受程序及其自动化

开发者应使用配置管理系统，提供配置管理文档，并满足以下要求：

a) **给产品标记唯一参照号；**
b) **配置管理文档描述用于唯一标识配置项的方法；**
c) **配置管理系统唯一标识所有配置项；**
d) **配置管理系统提供自动化的措施使得只能对配置项进行授权变更；**
e) **配置管理系统以自动化的方式支持产品的生产；**
f) **配置管理文档包括配置管理计划，配置管理计划应描述配置管理系统是如何应用于产品的开发的；**
g) **配置管理计划描述用来接受修改过的或新创建的作为产品组成部分的配置项的程序；**
h) **提供证据论证所有配置项都正在配置管理系统下进行维护，并论证配置管理系统的运行与配置管理计划是一致的。**

5.4.2.3.4 问题跟踪配置管理覆盖

开发者应向评估者提供产品配置项列表，满足以下要求：

a) 配置项列表包括：产品本身、安全保障要求的评估证据、产品的组成部分、实现表示和安全缺陷报告及其解决状态；
b) 配置项列表唯一标识配置项；
c) 对于每一个产品安全功能相关的配置项，配置项列表简要说明该配置项的开发者。

5.4.2.3.5 交付程序

开发者应将把产品或其部分交付给消费者的程序文档化，并满足以下要求：

a) 交付文档应描述在向消费者分发产品版本时，用以维护安全性所必需的所有程序；
b) 确认开发者在使用交付程序。

5.4.2.3.6 安全措施标识

开发者向评估者提供开发安全文档，满足以下要求：

a) 开发安全文档应描述在产品的开发环境中，保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的及其它方面的安全措施；
b) 确认安全措施在被使用。

5.4.2.3.7 开发者定义的生命周期模型

开发者应建立一个生命周期模型用于产品的开发和维护，提供生命周期定义文档，并满足以下要求：

a) 生命周期定义文档对用于开发和维护产品的模型进行描述；
b) 生命周期模型为产品的开发和维护提供必要的控制。

5.4.2.3.8 明确定义的开发工具

开发者应标识和明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义所有语句和实现用到的所有协定与命令，以及所有实现依赖选项的含义。

5.4.2.4 测试

5.4.2.4.1 覆盖分析

开发者应向评估者提供测试覆盖分析，并满足如下要求：

a) 测试覆盖分析论证测试文档中的测试与功能规范中的安全功能接口之间的对应性；
b) 测试覆盖分析论证已经对功能规范中的所有产品安全功能接口都进行了测试。

5.4.2.4.2 测试：安全执行模块

开发者应向评估者提供测试深度分析，并满足以下要求：

a) 测试深度分析论证测试文档中的测试与产品设计中的产品安全功能子系统、安全功能要求执行模块之间的一致性；
b) 测试深度分析论证产品设计中的所有产品安全功能子系统都已经进行过测试；
c) 测试深度分析论证产品设计中的安全功能要求执行模块都已经进行过测试。

5.4.2.4.3 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，标识要执行的测试并描述执行每个测试的方案，这些方案应包括对于其它测试结果的任何顺序依赖性；
b) 预期的测试结果，指出测试成功执行后的预期输出；
c) 实际的测试结果，确认和预期的测试结果的一致性。

5.4.2.4.4 独立测试—抽样

开发者应向评估者提供一组与开发者产品安全功能测试中同等的一系列资源，用于安全功能的抽样测试。

5.4.2.5 关注点脆弱性分析

开发者应提供适合测试的产品，并向评估者提供执行关注点脆弱性分析的相关资源，包括指导性文档、功能规范、产品设计、安全架构描述和实现表示。

5.5 性能要求

5.5.1 基本级

不做要求。

5.5.2 增强级

5.5.2.1 负载量

网络病毒监控系统的负载量视不同应用场景有所不同，具体指标要求如下：

a) 在只开启病毒检测功能的条件下，负载量应不低于线速的 60%；
b) 在开启全部安全功能的条件下，负载量应不低于线速的 40%。

6 测试评价方法

6.1 总体说明

测试评价方法与技术要求一一对应，它给出具体的测评方法来验证网络病毒监控系统是否达到技术要求中所提出的要求。它由测试环境、测试工具、测试方法和预期结果四个部分构成。

6.2 功能测试

6.2.1 测试环境与工具

网络病毒监控系统典型功能测试环境与工具参见附录B中B.1。

6.2.2 基本级

6.2.2.1 监测能力

6.2.2.1.1 应用协议支持

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统的应用协议策略；
   2) 检查网络病毒监控系统的病毒检测策略；
   3) 在内网、外网分别配置客户端和服务器，基于 HTTP 协议传输测试病毒样本；
   4) 在内网、外网分别配置客户端和服务器，基于 FTP 协议传输测试病毒样本；
   5) 在内网、外网分别配置客户端和服务器，基于 SMTP 协议传输测试病毒样本；
   6) 在内网、外网分别配置客户端和服务器，基于 POP3 协议传输测试病毒样本；
   7) 在内网、外网分别配置客户端和服务器，基于 SMB/CIFS 协议传输测试病毒样本；
b) 预期结果：
   1) 网络病毒监控系统应默认开启应用协议支持，并至少覆盖 5.2.1.1.2 中所述的常见应用协议之一；
   2) 网络病毒监控系统应默认开启病毒检测功能；
   3) 网络病毒监控系统能够对基于 HTTP 协议传输的测试病毒样本进行检测；
   4) 网络病毒监控系统能够对基于 FTP 协议传输的测试病毒样本进行检测；
   5) 网络病毒监控系统能够对基于 SMTP 协议传输的测试病毒样本进行检测；
   6) 网络病毒监控系统能够对基于 POP3 协议传输的测试病毒样本进行检测；
   7) 网络病毒监控系统能够对基于 SMB/CIFS 协议传输的测试病毒样本进行检测。

6.2.2.1.2 静态病毒防护

该项测试遵循以下测试方法：

a) 测试方法：
   1) 在内网、外网分别配置客户端，基于 HTTP、FTP、SMTP、POP3、SMB/CIFS 或其他应用协议中的一种或多种在客户端和服务器之间传输病毒样本基本库与流行病毒样本库中的病毒样本；
   2) 在内网、外网分别配置客户端，基于 HTTP、FTP、SMTP、POP3、SMB/CIFS 或其他应用协议中的一种或多种在客户端和服务器之间传输误报样本库中的样本。
b) 预期结果：
   1) 网络病毒监控系统对病毒样本基本库中的样本至少能检测其中的 90%；
   2) 网络病毒监控系统对流行病毒样本库中的样本至少能检测其中的 95%；
   3) 网络病毒监控系统不会对误报样本库中的样本进行检测。

6.2.2.1.3 逃避检测防护

该项测试遵循以下测试方法：

a) 测试方法：
   1) 配置网络病毒监控系统开启对压缩格式文件的检测功能；
   2) 将病毒样本基本库和流行病毒样本库中网络病毒监控系统能够检测的病毒样本进行一层和多层压缩；
   3) 在内网、外网分别配置客户端和服务器，在客户端和服务器之间传输压缩格式的病毒样本。
b) 预期结果：网络病毒监控系统能够对压缩格式的病毒样本进行检测。

6.2.2.1.4 多种类型网络应用场景支持

该项测试遵循以下测试方法：

a) 测试方法：

1） 配置内部网络、外部网络地址均为 IPv4 类型地址，进行 6.2.2.1.1 ～ 6.2.2.1.3 测试；
2） 配置内部网络、外部网络地址均为 IPv6 类型地址，进行 6.2.2.1.1 ～ 6.2.2.1.3 测试；
3） 配置外部网络为 IPv4 地址，内部网络为 IPv6 地址，进行 6.2.2.1.1 ～ 6.2.2.1.3 测试。

b） 预期结果：
1） 内部网络、外部网络地址均为 IPv4 类型地址时，网络病毒监控系统能够通过 6.2.2.1.1 ～ 6.2.2.1.3 测试；
2） 内部网络、外部网络地址均为 IPv6 类型地址时，网络病毒监控系统能够通过 6.2.2.1.1 ～ 6.2.2.1.3 测试；
3） 外部网络为 IPv4 地址，内部网络为 IPv6 地址，网络病毒监控系统能够通过 6.2.2.1.1 ～ 6.2.2.1.3 测试。

6.2.2.2 监控策略

6.2.2.2.1 策略自定义

该项测试遵循以下测试方法：

a） 测试方法：
1） 根据 5.2.1.1.1 ～ 5.2.1.1.7 中的功能要求添加病毒监控策略；
2） 进行 6.2.2.1.2 测试；
3） 根据 5.2.1.1.1 ～ 5.2.1.1.7 中的功能要求修改刚添加的病毒监控策略；
4） 进行 6.2.2.1.2 测试；
5） 根据 5.2.1.1.1 ～ 5.2.1.1.7 中的功能要求删除刚修改的病毒监控策略；
6） 进行 6.2.2.1.2 测试。

b） 预期结果：网络病毒监控系统能够根据自定义的策略完成相应的病毒检测和告警。

6.2.2.2.2 策略初始模版

该项测试遵循以下测试方法：

a） 测试方法：
1） 检查网络病毒监控系统的应用协议策略；
2） 检查网络病毒监控系统的病毒检测策略。

b） 预期结果：
1） 网络病毒监控系统应默认开启应用协议支持，并至少覆盖 5.2.2.1.2 中所述的常见应用协议之一；
2） 网络病毒监控系统应默认开启病毒检测功能。

6.2.2.3 响应处理

6.2.2.3.1 病毒检测

该项测试遵循以下测试方法：

a） 测试方法：
1） 配置网络病毒监控系统的病毒响应处理策略为检测和告警；
2） 进行 6.2.2.1.2 的测试。

b） 预期结果：网络病毒监控系统能够对病毒样本文件进行告警。

6.2.2.3.2 告警信息

该项测试遵循以下测试方法：

a) 测试方法：
   1) 开启网络病毒监控系统的告警功能；
   2) 进行 5.2.1.1.1 ～ 5.2.1.1.7 的各项测试；
   3) 查看网络病毒监控系统告警信息。
b) 预期结果：
   1) 网络病毒监控系统应具有告警功能；
   2) 网络病毒监控系统告警信息中应包括 5.2.1.3.2 中要求的各项信息。

6.2.2.3.3 告警方式

该项测试遵循以下测试方法：

a) 测试方法：
   1) 配置网络病毒监控系统的告警方式；
   2) 进行 5.2.1.1.1 ～ 5.2.1.1.7 的各项测试；
   3) 查看网络病毒监控系统的管理界面，查收报警邮件，查收短信或其他可以收取告警信息的设备或系统。
b) 预期结果：
   1) 网络病毒监控系统至少具有屏幕实时提示、邮件告警、短信告警和声音报警等告警方式的一种或多种；
   2) 网络病毒监控系统能够通过具有的告警方式向用户发送告警信息。

6.2.2.3.4 事件记录

该项测试遵循以下测试方法：

a) 测试方法：
   1) 配置网络病毒监控系统，开启安全事件日志记录功能；
   2) 进行 5.2.1.1.1 ～ 5.2.1.1.7 的各项测试；
   3) 查看网络病毒监控系统的安全事件日志；
   4) 拔掉网络病毒监控系统的电源，再重新接上电源，开启网络病毒监控系统，检查网络病毒监控系统的安全事件日志是否完整，是否丢失了断电前的日志信息；
   5) 检查事件日志存储空间配置，并配置存储空间报警阈值。
b) 预期结果：
   1) 网络病毒监控系统具有安全事件日志，并能够记录病毒传播行为、恶意 URL 访问等安全事件的详细信息；
   2) 断电重启后，网络病毒监控系统的安全事件日志不会丢失；
   3) 安全事件存储空间达到报警阈值时，能够通知授权管理员。

6.2.2.4 报表和统计

6.2.2.4.1 报表生成

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统的报表生成配置；
   2) 使用网络病毒监控系统提供的缺省报表模版生成报表；

3) 配置网络病毒监控系统的自定义报表模版；
4) 使用自定义报表模版生成报表；
5) 检查报表内容是否与模版匹配。

b) 预期结果：
1) 网络病毒监控系统具有报表生成功能；
2) 网络病毒监控系统提供缺省报表模版；
3) 网络病毒监控系统能够按缺省报表模版生成报表；
4) 网络病毒监控系统能够按用户自定义的报表模版生成报表；
5) 报表内容与报表模版匹配。

6.2.2.4.2 报表导出

该项测试遵循以下测试方法：

a) 测试方法：
1) 配置网络病毒监控系统的报表导出设置，导出格式为 DOC、PDF、HTML、XLS、CSV、XML 等一种或多种；
2) 导出报表；
3) 打开导出的报表，检查内容是否完整准确。

b) 预期结果：
1) 网络病毒监控系统具有报表导出功能，并能够导出格式为 DOC、PDF、HTML、XLS、CSV、XML 等一种或多种报表文件；
2) 网络病毒监控系统能够正常导出报表文件；
3) 导出的报表文件内容完整准确；
4) 网络病毒监控系统能够按用户自定义的报表模版生成报表；
5) 报表内容与报表模版匹配。

6.2.2.4.3 统计功能

该项测试遵循以下测试方法：

a) 测试方法：
1) 检查网络病毒监控系统的安全事件统计功能；
2) 配置统计条件为基于 HTTP 协议的病毒传播事件；
3) 查看统计结果是否与统计条件相符。

b) 预期结果：
1) 网络病毒监控系统具有安全事件统计功能；
2) 网络病毒监控系统能够根据统计条件输出正确的统计结果。

6.2.2.5 故障信息告警

该项测试遵循以下测试方法：

a) 测试方法：
1) 人为造成网络病毒监控系统产品的一种软件故障；
2) 人为造成网络病毒监控系统产品的一种硬件故障。

b) 预期结果：产品通过屏幕实时提示、邮件告警、短信告警、声音告警等一种或多种方式进行故障告警。

6.2.2.6 升级能力

该项测试遵循以下测试方法：

a) 测试方法：
   1) 开启网络病毒监控系统的自动升级功能，并配置自动更新时间；
   2) 通过手动方式启动网络病毒监控系统升级；
   3) 通过手动方式导入离线升级文件；
   4) 检查系统版本、病毒库版本等信息；
b) 预期结果：网络病毒监控系统能够通过自动和手动方式升级到最新版本。

6.2.3 增强级

6.2.3.1 监测能力

6.2.3.1.1 应用协议支持

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统的应用协议策略；
   2) 检查网络病毒监控系统的病毒检测策略；
   3) 在内网、外网分别配置客户端和服务器，基于 HTTP 协议传输测试病毒样本；
   4) 在内网、外网分别配置客户端和服务器，基于 FTP 协议传输测试病毒样本；
   5) 在内网、外网分别配置客户端和服务器，基于 SMTP 协议传输测试病毒样本；
   6) 在内网、外网分别配置客户端和服务器，基于 POP3 协议传输测试病毒样本；
   7) 在内网、外网分别配置客户端和服务器，基于 SMB/CIFS 协议传输测试病毒样本；
   8) 在内网、外网分别配置客户端和服务器，基于其他应用协议传输测试病毒样本。
b) 预期结果：
   1) 网络病毒监控系统应默认开启应用协议支持，并至少覆盖 5.2.2.1.2 中所述的常见应用协议之一；
   2) 网络病毒监控系统应默认开启病毒检测功能；
   3) 网络病毒监控系统能够对基于 HTTP 协议传输的测试病毒样本进行检测；
   4) 网络病毒监控系统能够对基于 FTP 协议传输的测试病毒样本进行检测；
   5) 网络病毒监控系统能够对基于 SMTP 协议传输的测试病毒样本进行检测；
   6) 网络病毒监控系统能够对基于 POP3 协议传输的测试病毒样本进行检测；
   7) 网络病毒监控系统能够对基于 SMB/CIFS 协议传输的测试病毒样本进行检测；
   8) 网络病毒监控系统能够对基于其他应用协议传输的测试病毒样本进行检测。

6.2.3.1.2 静态病毒防护

该项测试遵循以下测试方法：

a) 测试方法：
   1) 在内网、外网分别配置客户端，基于 HTTP、FTP、SMTP、POP3、SMB/CIFS 或其他应用协议中的一种或多种在客户端和服务器之间传输病毒样本基本库与流行病毒样本库中的病毒样本；
   2) 在内网、外网分别配置客户端，基于 HTTP、FTP、SMTP、POP3、SMB/CIFS 或其他应用协议中的一种或多种在客户端和服务器之间传输误报样本库中的样本。

b) 预期结果：

1) 网络病毒监控系统对病毒样本基本库中的样本至少能检测其中的 90%；

2) 网络病毒监控系统对流行病毒样本库中的样本至少能检测其中的 95%；

3) 网络病毒监控系统不会对误报样本库中的样本进行检测。

6.2.3.1.3 动态病毒防护

该项测试遵循以下测试方法：

a) 测试方法：

1) 在内网中配置若干台感染机，依次激活可执行恶意软件样本库中的样本；

2) 在外网配置服务器，部署恶意网页脚本样本库中的样本，用内网中的客户端访问服务器上的样本。

b) 预期结果：

1) 网络病毒监控系统对可执行恶意软件样本库中的样本至少能检测其中的 90%；

2) 网络病毒监控系统对恶意网页脚本样本库中的样本至少能检测其中的 90%。

6.2.3.1.4 逃避检测防护

该项测试遵循以下测试方法：

a) 测试方法：

1) 配置网络病毒监控系统开启对压缩格式文件**和加壳文件**的检测功能；

2) 将病毒样本基本库和流行病毒样本库中网络病毒监控系统能够检测的病毒样本进行一层和多层压缩；

3) 将病毒样本基本库和流行病毒样本库中网络病毒监控系统能够检测的病毒样本进行加壳；

4) 在内网、外网分别配置客户端和服务器，在客户端和服务器之间传输压缩格式**和加壳格式**的病毒样本；

b) 预期结果：

1) 网络病毒监控系统能够对压缩格式的病毒样本进行检测；

2) 网络病毒监控系统对加壳格式病毒样本进行检测。

6.2.3.1.5 恶意 URL 检测

该项测试遵循以下测试方法：

a) 测试方法：

1) 配置网络病毒监控系统的安全策略，开启 URL 检测功能；

2) 在内网客户端访问含有病毒、木马等恶意软件的恶意 URL；

b) 预期结果：网络病毒监控系统能够对含有病毒、木马等恶意软件的恶意 URL 进行告警。

6.2.3.1.6 多种类型网络应用场景支持

该项测试遵循以下测试方法：

a) 测试方法：

1) 配置内部网络、外部网络地址均为 IPv4 类型地址，进行 6.2.3.1.1 ～ 6.2.3.1.5 测试；

2) 配置内部网络、外部网络地址均为 IPv6 类型地址，进行 6.2.3.1.1 ～ 6.2.3.1.5 测试；

3) 配置外部网络为 IPv4 地址，内部网络为 IPv6 地址，进行 6.2.3.1.1 ～ 6.2.3.1.5 测试；

b) 预期结果：

1） 内部网络、外部网络地址均为 IPv4 类型地址时，网络病毒监控系统能够通过 6.2.3.1.1 ～ 6.2.3.1.5 测试；
2） 内部网络、外部网络地址均为 IPv6 类型地址时，网络病毒监控系统能够通过 6.2.3.1.1 ～ 6.2.3.1.5 测试；
3） 外部网络为 IPv4 地址，内部网络为 IPv6 地址，网络病毒监控系统能够通过 6.2.3.1.1 ～ 6.2.3.1.5 测试。

6.2.3.2 监控策略

6.2.3.2.1 策略自定义

该项测试遵循以下测试方法：

a） 测试方法：
1） 根据 5.2.2.1.1 ～ 5.2.2.1.7 中的功能要求添加病毒监控策略；
2） 进行 6.2.3.1.3 测试；
3） 根据 5.2.2.1.1 ～ 5.2.2.1.7 中的功能要求修改刚添加的病毒监控策略；
4） 进行 6.2.3.1.3 测试；
5） 根据 5.2.2.1.1 ～ 5.2.2.1.7 中的功能要求删除刚修改的病毒监控策略；
6） 进行 6.2.3.1.3 测试。

b） 预期结果：网络病毒监控系统能够根据自定义的策略完成相应的病毒检测和告警。

6.2.3.2.2 策略初始模版

该项测试遵循以下测试方法：

a） 测试方法：
1） 检查网络病毒监控系统的应用协议策略；
2） 检查网络病毒监控系统的病毒检测策略。

b） 预期结果：
1） 网络病毒监控系统应默认开启应用协议支持，并至少覆盖 5.2.2.1.2 中所述的常见应用协议之一；
2） 网络病毒监控系统应默认开启病毒检测功能。

6.2.3.3 响应处理

6.2.3.3.1 病毒检测

该项测试遵循以下测试方法：

a） 测试方法：
1） 配置网络病毒监控系统的病毒响应处理策略为检测和告警；
2） 进行 6.2.3.1.2 的测试。

b） 预期结果：网络病毒监控系统能够对病毒样本文件进行告警。

6.2.3.3.2 病毒捕获

该项测试遵循以下测试方法：

a） 测试方法：
1） 配置网络病毒监控系统的病毒响应处理策略为检测并捕获；
2） 进行 6.2.3.1.2 的测试；

3) **下载捕获的病毒样本文件；**
4) **对下载的病毒样本文件与原始病毒样本文件进行一致性校验。**

b) **预期结果：**
1) **网络病毒监控系统能够对病毒样本文件进行告警，并将病毒样本文件存储在受限制存储区域中；**
2) **网络病毒监控系统捕获的病毒样本文件与原始病毒样本文件一致。**

6.2.3.3.3 告警信息

该项测试遵循以下测试方法：

a) 测试方法：
1) 开启网络病毒监控系统的告警功能；
2) 进行 5.2.2.1.1 ～ 5.2.2.1.7 的各项测试；
3) 查看网络病毒监控系统告警信息。

b) 预期结果：
1) 网络病毒监控系统应具有告警功能；
2) 网络病毒监控系统告警信息中应包括 5.2.2.3.4 中要求的各项信息。

6.2.3.3.4 告警方式

该项测试遵循以下测试方法：

a) 测试方法：
1) 配置网络病毒监控系统的告警方式；
2) 进行 5.2.2.1.1 ～ 5.2.2.1.7 的各项测试；
3) 查看网络病毒监控系统的管理界面，查收报警邮件，查收短信或其他可以收取告警信息的设备或系统。

b) 预期结果：
1) 网络病毒监控系统至少具有屏幕实时提示、邮件告警、短信告警和声音报警等告警方式的一种或多种；
2) 网络病毒监控系统能够通过具有的告警方式向用户发送告警信息。

6.2.3.3.5 事件记录

该项测试遵循以下测试方法：

a) 测试方法：
1) 配置网络病毒监控系统，开启安全事件日志记录功能；
2) 进行 5.2.2.1.1 ～ 5.2.2.1.7 的各项测试；
3) 查看网络病毒监控系统的安全事件日志；
4) 拔掉网络病毒监控系统的电源，再重新接上电源，开启网络病毒监控系统，检查网络病毒监控系统的安全事件日志是否完整，是否丢失了断电前的日志信息；
5) 检查事件日志存储空间配置，并配置存储空间报警阈值。

b) 预期结果：
1) 网络病毒监控系统具有安全事件日志，并能够记录病毒传播行为、恶意 URL 访问等安全事件的详细信息；
2) 断电重启后，网络病毒监控系统的安全事件日志不会丢失；
3) 安全事件存储空间达到报警阈值时，能够通知授权管理员。

6.2.3.4 报表和统计

6.2.3.4.1 报表生成

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统的报表生成配置；
   2) 使用网络病毒监控系统提供的缺省报表模版生成报表；
   3) 配置网络病毒监控系统的自定义报表模版；
   4) 使用自定义报表模版生成报表；
   5) 检查报表内容是否与模版匹配。
b) 预期结果：
   1) 网络病毒监控系统具有报表生成功能；
   2) 网络病毒监控系统提供缺省报表模版；
   3) 网络病毒监控系统能够按缺省报表模版生成报表；
   4) 网络病毒监控系统能够按用户自定义的报表模版生成报表；
   5) 报表内容与报表模版匹配。

6.2.3.4.2 报表导出

该项测试遵循以下测试方法：

a) 测试方法：
   1) 配置网络病毒监控系统的报表导出设置，导出格式为 DOC、PDF、HTML、XLS、CSV、XML 等一种或多种；
   2) 导出报表；
   3) 打开导出的报表，检查内容是否完整准确。
b) 预期结果：
   1) 网络病毒监控系统具有报表导出功能，并能够导出格式为 DOC、PDF、HTML、XLS、CSV、XML 等一种或多种报表文件；
   2) 网络病毒监控系统能够正常导出报表文件；
   3) 导出的报表文件内容完整准确；
   4) 网络病毒监控系统能够按用户自定义的报表模版生成报表；
   5) 报表内容与报表模版匹配。

6.2.3.4.3 统计功能

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统的安全事件统计功能；
   2) 配置统计条件为基于 HTTP 协议的病毒传播事件；
   3) 查看统计结果是否与统计条件相符。
b) 预期结果：
   1) 网络病毒监控系统具有安全事件统计功能；
   2) 网络病毒监控系统能够根据统计条件输出正确的统计结果。

6.2.3.5 异常流量处理

该项测试遵循以下测试方法：

a) 测试方法：

1) 按照图 1 配置测试环境，测试仪的两个接口将分别接入内部网络和外部网络；

2) 配置测试仪，发送碎片包、畸形报文和其他类型的异常流量；

3) 进行 6.2.3.1.2 测试。

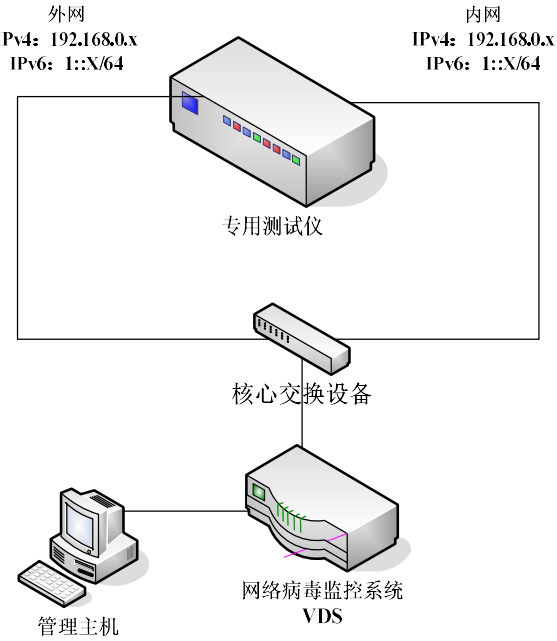

图 1 异常流量处理测试环境示意图

b) 预期结果：网络病毒监控系统能够正常完成对病毒样本的检测。

6.2.3.6 故障信息告警

该项测试遵循以下测试方法：

a) 测试方法：

1) 人为造成网络病毒监控系统产品的一种软件故障；

2) 人为造成网络病毒监控系统产品的一种硬件故障；

b) 预期结果：产品通过屏幕实时提示、邮件告警、短信告警、声音告警等一种或多种方式进行故障告警。

6.2.3.7 升级能力

该项测试遵循以下测试方法：

a) 测试方法：

1) 开启网络病毒监控系统的自动升级功能，并配置自动更新时间；

2) 通过手动方式启动网络病毒监控系统升级；

3) 通过手动方式导入离线升级文件；

4) 检查系统版本、病毒库版本等信息；

5) 查看网络病毒监控系统是否支持增量升级功能；

6) 通过自动或手动方式进行增量升级；

7) 检查系统版本、病毒库版本等信息。

b) 预期结果：

1) 网络病毒监控系统能够通过自动和手动方式升级到最新版本；

2) 网络病毒监控系统能够通过增量升级方式升级到最新版本。

6.2.3.8 协同联动能力

该项测试遵循以下测试方法：

a) 测试方法：

1) 以防病毒网关为例，进行测试；

2) 配置网络病毒监控系统的联动策略，并设定认证方式；

3) 内部网络客户端从外部网络服务器上下载病毒样本文件，检查防病毒网关是否能够接收网络病毒监控系统的报警，并阻断样本传输。

b) 预期结果：防病毒网关及时响应受信任的并通过认证的网络病毒监控系统的报警信息，并阻断该病毒样本的传输。

6.3 安全性测试

6.3.1 基本级

6.3.1.1 标识与鉴别

6.3.1.1.1 管理员标识

该项测试遵循以下测试方法：

a) 测试方法：

1) 检查网络病毒监控系统的授权管理员管理功能，是否有分组、权限分配功能；

2) 按网络病毒监控系统提供的默认安全属性创建一个授权管理员；

3) 检查授权管理员标识是否唯一；

b) 预期结果：

1) 网络病毒监控系统具有较为完整的授权管理员管理功能，具有分组、权限分配功能；

2) 网络病毒监控系统可以创建一个具有默认安全属性的授权管理员用户；

3) 授权管理员标识为唯一。

6.3.1.1.2 身份鉴别

该项测试遵循以下测试方法：

a) 测试方法：

1) 检查网络病毒监控系统是否有身份鉴别功能；

2) 使用网络病毒监控系统相关安全功能前管理员是否需要输入凭据；

3) 检查网络病毒监控系统的身份鉴别数据是否能够由未经授权的管理员查阅或修改；

4) 输入正确的凭据组合，产品是否能够允许管理员登录；

5) 输入错误的凭据组合，产品是否能够允许管理员登录。

b) 预期结果：

1) 网络病毒监控系统具有用户身份鉴别功能；

2) 管理员必须输入合法凭据才能使用网络病毒监控系统的相关安全功能；

3) 网络病毒监控系统的用户身份鉴别数据不会被未经授权的管理员查阅或修改；

4) 对于正确的凭据组合，网络病毒监控系统能够允许管理员正常登录；

5） 对于错误的凭据组合，网络病毒监控系统能够拒绝管理员登录。

6.3.1.2 安全管理

6.3.1.2.1 安全功能管理

该项测试遵循以下测试方法：

a） 测试方法：

1） 使用授权管理员的合法凭据登录网络病毒监控系统；
2） 查看、修改网络病毒监控系统的相关安全属性；
3） 启动、关闭网络病毒监控系统的全部或部分安全功能；
4） 新增、修改网络病毒监控系统的恶意软件监控策略等各种安全策略。

b） 预期结果：

1） 授权管理员能够查看、修改相关安全属性；
2） 授权管理员能够启动、关闭网络病毒监控系统的全部或部分安全功能；
3） 授权管理员能够新增、修改网络病毒监控系统的病毒监控策略等各种安全策略。

6.3.1.2.2 安全管理方式

该项测试遵循以下测试方法：

a） 测试方法：

1） 检查网络病毒监控系统是否有 console 接口；
2） 使用 console 接口连接到网络病毒监控系统，对网络病毒监控系统进行管理；
3） 检查网络病毒监控系统是否有可供远程管理的网络接口，并为其分配网络地址；
4） 通过远程管理接口对网络病毒监控系统进行管理。

b） 预期结果：

1） 网络病毒监控系统具有 console 接口，并能够通过 console 接口对网络病毒监控系统进行管理；
2） 网络病毒监控系统具有远程管理接口，并能够通过网络远程对网络病毒监控系统进行管理。

6.3.1.3 审计日志

6.3.1.3.1 审计日志生成

该项测试遵循以下测试方法：

a） 测试方法：

1） 检查并开启网络病毒监控系统的审计日志功能；
2） 分别使用正确和错误的管理员身份鉴别凭据登录网络病毒监控系统；
3） 对安全策略进行修改；
4） 增加、删除管理员，并修改管理员账户信息；
5） 多次使用不符合鉴别条件的用户凭据登录网络病毒监控系统，直到网络病毒监控系统终止会话连接；
6） 对事件记录日志、审计日志进行导出和删除等操作；
7） 进行除 1）～ 6）以外的其他操作；
8） 查看审计日志。

b） 预期结果：

1) 网络病毒监控系统具有审计日志生成功能；
2) 网络病毒监控系统的审计日志能够记录用户登录和失败事件；
3) 网络病毒监控系统的审计日志能够记录用户对安全策略的更改事件；
4) 网络病毒监控系统的审计日志能够记录管理员的增加、删除和属性修改事件；
5) 网络病毒监控系统的审计日志能够记录因鉴别失败次数超出设定值，导致会话连接终止的事件；
6) 网络病毒监控系统的审计日志能够记录对事件日志和审计日志的操作事件；
7) 网络病毒监控系统的审计日志能够记录管理员的其他操作；
8) 网络病毒监控系统的每一条审计日志至少包括事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

6.3.1.3.2 审计日志存储

该项测试遵循以下测试方法：

a) 测试方法：
   1) 查看网络病毒监控系统的审计日志；
   2) 突然切断网络病毒监控系统的电源供应；
   3) 恢复网络病毒监控系统的电源供应，查看网络病毒监控系统的审计日志；
   4) 对比断电前后的审计日志。
b) 预期结果：
   1) 断电重启后网络病毒监控系统的审计日志不会丢失；
   2) 审计日志默认最低保存期限不少于六个月。

6.3.1.3.3 审计日志管理

该项测试遵循以下测试方法：

a) 测试方法：
   1) 使用非授权管理员身份访问审计日志；
   2) 使用授权管理员身份访问审计日志；
   3) 输入查询条件，查询符合条件的审计日志；
   4) 导出审计日志并保存；
   5) 打开读取导出的审计日志文件，并与网络病毒监控系统中的审计日志记录对比。
b) 预期结果：
   1) 网络病毒监控系统只允许授权管理员访问审计日志；
   2) 授权管理员能够根据查询条件查询符合条件的审计日志；
   3) 授权管理员能够导出符合条件的审计日志，并保存为文件；
   4) 导出的审计日志文件内容与网络病毒监控系统中的审计日志记录内容相符。

6.3.2 增强级

6.3.2.1 标识与鉴别

6.3.2.1.1 用户标识

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统的授权管理员管理功能，是否有分组、权限分配功能；

2) 按网络病毒监控系统提供的默认安全属性创建一个授权管理员；
3) 检查授权管理员标识是否唯一。

b) 预期结果：
1) 网络病毒监控系统具有较为完整的用户管理功能，具有用户分组、权限分配功能；
2) 网络病毒监控系统可以创建一个具有默认安全属性的管理员用户；
3) 授权管理员标识为唯一。

6.3.2.1.2 身份鉴别

该项测试遵循以下测试方法：

a) 测试方法：
1) 检查网络病毒监控系统是否有身份鉴别功能；
2) 使用网络病毒监控系统相关安全功能前管理员是否需要输入凭据；
3) 检查网络病毒监控系统的身份鉴别数据是否能够由未经授权的用户查阅或修改；
4) 多次尝试输入错误的鉴别凭据，产品能否提示并终止管理员的访问；
5) 检查网络病毒监控系统是否对同一管理员采用两种或两种以上组合的用户身份鉴别方式；
6) 输入正确的凭据组合，产品是否能够允许用户登录；
7) 输入错误的凭据组合，产品是否能够允许用户登录。

b) 预期结果：
1) 网络病毒监控系统具有用户身份鉴别功能；
2) 用户必须输入合法凭据才能使用网络病毒监控系统的相关安全功能；
3) 网络病毒监控系统的用户身份鉴别数据不会被未经授权的用户查阅或修改；
4) 多次错误的鉴别凭据将导致用户被终止访问网络病毒监控系统；
5) 网络病毒监控系统对同一用户采用了两种或两种以上组合的用户身份鉴别方式；
6) 对于正确的凭据组合，网络病毒监控系统能够允许用户正常登录；
7) 对于错误的凭据组合，网络病毒监控系统能够拒绝用户登录。

6.3.2.2 安全管理

6.3.2.2.1 安全功能管理

该项测试遵循以下测试方法：

a) 测试方法：
1) 使用授权管理员的合法凭据登录网络病毒监控系统；
2) 查看、修改网络病毒监控系统的相关安全属性；
3) 启动、关闭网络病毒监控系统的全部或部分安全功能；
4) 新增、修改网络病毒监控系统的病毒监控策略等各种安全策略。

b) 预期结果：
1) 授权管理员能够查看、修改相关安全属性；
2) 授权管理员能够启动、关闭网络病毒监控系统的全部或部分安全功能；
3) 授权管理员能够新增、修改网络病毒监控系统的病毒监控策略等各种安全策略。

6.3.2.2.2 安全角色管理

该项测试遵循以下测试方法：

a) **测试方法：**
   1) **检查网络病毒监控系统是否有至少两种不同权限的管理员角色；**
   2) **检查网络病毒监控系统是否能够根据不同的功能模块定义不同的权限角色；**
   3) **为用户分配相应的权限角色；**
   4) **检查用户是否具有与其角色相符的权限。**
b) **预期结果：**
   1) **网络病毒监控系统具有至少两种不同权限的管理员角色；**
   2) **网络病毒监控系统能够根据不同的功能模块定义不同的权限角色；**
   3) **角色分配后，用户具有与其角色相符的权限。**

6.3.2.2.3 安全管理方式

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查网络病毒监控系统是否有 console 接口；
   2) 使用 console 接口连接到网络病毒监控系统，对网络病毒监控系统进行管理；
   3) 检查网络病毒监控系统是否有可供远程管理的网络接口，并为其分配网络地址；
   4) 通过远程管理接口对网络病毒监控系统进行管理；
   5) **检查远程管理客户机与网络病毒监控系统的通讯过程是否采用加密方式。**
b) 预期结果：
   1) 网络病毒监控系统具有 console 接口，并能够通过 console 接口对网络病毒监控系统进行管理；
   2) 网络病毒监控系统具有远程管理接口，并能够通过网络远程对网络病毒监控系统进行管理；
   3) **远程管理客户机与网络病毒监控系统之间的通讯过程采用加密方式。**

6.3.2.2.4 远程保密传输

该项测试遵循以下测试方法：

a) **测试方法：**
   1) **检查网络病毒监控系统是否由使用网络进行通讯的若干组件构成；**
   2) **检查网络病毒监控系统组件间的网络通讯是否通过加密方式。**
b) **预期结果：网络病毒监控系统各组件间的网络通讯均采用加密方式。**

6.3.2.2.5 可信管理主机

该项测试遵循以下测试方法：

a) **测试方法：**
   1) **检查网络病毒监控系统能否限制远程管理主机的 IP 地址；**
   2) **使用符合限制条件的远程主机连接网络病毒监控系统的管理控制台；**
   3) **使用不符合限制条件的远程主机连接网络病毒监控系统的管理控制台；**
b) **预期结果：**
   1) **网络病毒监控系统能够限制远程管理主机的 IP 地址；**
   2) **网络病毒监控系统允许符合限制条件的远程主机连接到管理控制台；**
   3) **网络病毒监控系统拒绝不符合限制条件的远程主机连接到管理控制台。**

6.3.2.2.6 数据完整性

该项测试遵循以下测试方法：

a) **测试方法：**
   1) **使用破坏性修改的授权管理员授权文件对网络病毒监控系统进行激活授权操作；**
   2) **将经过破坏性修改的授权管理员策略配置文件导入网络病毒监控系统；**
   3) **使用经过破坏性修改的系统升级包对网络病毒监控系统进行系统软件升级；**
   4) **使用经过破坏性修改的病毒特征库升级包对网络病毒监控系统进行病毒特征库升级。**
b) **预期结果：**
   1) **网络病毒监控系统能够对导入的授权管理员信息、策略信息、关键程序和病毒特征库进行数据完整性校验；**
   2) **网络病毒监控系统能够根据将完整性校验结果提供给授权管理员。**

6.3.2.2.7 安全支撑系统

该项测试遵循以下测试方法：

a) **测试方法：**
   1) **使用端口扫描器对网络病毒监控系统进行服务端口扫描；**
   2) **使用 telnet、nc 等程序访问网络病毒监控系统开放的网络端口；**
   3) **网络病毒监控系统对外提供的网络服务与其功能说明是否相符；**
   4) **使用漏洞扫描系统和网络攻击仿真测试仪对网络病毒监控系统进行漏洞检测和攻击测试。**
b) **预期结果：**
   1) **网络病毒监控系统不提供多余的网络服务；**
   2) **网络病毒监控系统不含导致产品权限丢失、拒绝服务等的安全漏洞。**

6.3.2.3 审计日志

6.3.2.3.1 审计日志生成

该项测试遵循以下测试方法：

a) 测试方法：
   1) 检查并开启网络病毒监控系统的审计日志功能；
   2) 分别使用正确和错误的管理员身份鉴别凭据登录网络病毒监控系统；
   3) 对安全策略进行修改；
   4) 增加、删除管理员，并修改管理员账户信息；
   5) 多次使用不符合鉴别条件的用户凭据登录网络病毒监控系统，直到网络病毒监控系统终止会话连接；
   6) 对事件记录日志、审计日志进行导出和删除等操作；
   7) 进行除 1）～ 6）以外的其他操作；
   8) 查看审计日志。
b) 预期结果：
   1) 网络病毒监控系统具有审计日志生成功能；
   2) 网络病毒监控系统的审计日志能够记录用户登录和失败事件；
   3) 网络病毒监控系统的审计日志能够记录用户对安全策略的更改事件；
   4) 网络病毒监控系统的审计日志能够记录管理员的增加、删除和属性修改事件；

5) 网络病毒监控系统的审计日志能够记录因鉴别失败次数超出设定值，导致会话连接终止的事件；
6) 网络病毒监控系统的审计日志能够记录对事件日志和审计日志的操作事件；
7) 网络病毒监控系统的审计日志能够记录管理员的其他操作；
8) 网络病毒监控系统的每一条审计日志至少包括事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

6.3.2.3.2 审计日志存储

该项测试遵循以下测试方法：

a) 测试方法：
   1) 查看网络病毒监控系统的审计日志；
   2) 突然切断网络病毒监控系统的电源供应；
   3) 恢复网络病毒监控系统的电源供应，查看网络病毒监控系统的审计日志；
   4) 对比断电前后的审计日志。
b) 预期结果：
   1) 断电重启后网络病毒监控系统的审计日志不会丢失；
   2) 审计日志默认最低保存期限不少于六个月。

6.3.2.3.3 审计日志管理

该项测试遵循以下测试方法：

a) 测试方法：
   1) 使用非授权管理员身份访问审计日志；
   2) 使用授权管理员身份访问审计日志；
   3) 输入查询条件，查询符合条件的审计日志；
   4) 导出审计日志并保存；
   5) 打开读取导出的审计日志文件，并与网络病毒监控系统中的审计日志记录对比。
b) 预期结果：
   1) 网络病毒监控系统只允许授权管理员访问审计日志；
   2) 授权管理员能够根据查询条件查询符合条件的审计日志；
   3) 授权管理员能够导出符合条件的审计日志，并保存为文件；
   4) 导出的审计日志文件内容与网络病毒监控系统中的审计日志记录内容相符。

6.4 安全保障评估

6.4.1 基本级

6.4.1.1 开发

6.4.1.1.1 安全架构描述

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查产品安全功能安全架构描述文档，确认是否满足 5.4.1.1.1 的要求；
b) 预期结果：产品安全功能安全架构描述文档符合 5.4.1.1.1 的要求。

6.4.1.1.2 安全执行功能规范

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的功能规范文档，确认是否满足 5.4.1.1.2 的要求；

b) 预期结果：开发者提供了功能规范文档，并且文档符合 5.4.1.1.2 的要求。

6.4.1.1.3 基础设计

该项评估应遵循以下评估方法：

a) 评估方法如下：

1) 评估者审查开发者提供的产品设计文档，确认是否满足 5.4.1.1.3 中对设计文档的要求；

2) 评估者审查映射关系说明，确认是否满足 5.4.1.1.3 中对映射关系的要求；

3) 评估者确认设计是否所有安全功能要求的正确且完备的实例。

b) 预期结果如下：

1） 开发者提供的产品设计文档，满足 5.4.1.1.3 中对设计文档的要求；

2） 映射关系说明满足 5.4.1.1.3 中对映射关系的要求；

3） 能够确认设计是所有安全功能要求的正确且完备的实例。

6.4.1.2 指导性文档

6.4.1.2.1 准备程序

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查开发者提供的准备程序，确认是否满足 5.4.1.2.1 的要求；

2） 评估者运用准备程序确认产品运行是否能被安全的准备。

b) 预期结果如下：

1） 开发者提供的准备程序，满足 5.4.1.2.1 的要求；

2） 运用准备程序能够做好产品安全运行的准备。

6.4.1.2.2 操作用户指南

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的操作用户指南，确认是否满足 5.4.1.2.2 的要求；

b) 预期结果：开发者提供的操作用户指南，满足 5.4.1.2.2 的要求。

6.4.1.3 生命周期支持

6.4.1.3.1 配置管理系统的使用

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者审查确认开发者是否使用了配置管理系统；

2） 评估者审查开发者提供的配置管理文档，确认是否满足 5.4.1.3.1 的要求。

b) 预期结果如下：

1） 能够确认开发者使用了配置管理系统；

2） 开发者提供的配置管理文档，满足 5.4.1.3.1 的要求。

6.4.1.3.2 部分产品配置管理覆盖

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的产品配置项列表，确认是否满足 5.4.1.3.2 的要求；
b) 预期结果：开发者提供的产品配置项列表，满足 5.4.1.3.2 的要求。

6.4.1.3.3 交付程序

该项评估应遵循以下评估方法：
a) 评估方法如下：
   1） 评估者审查开发者提供的交付程序文档，确认是否满足 5.4.1.3.3 的要求；
   2） 评估者审查确认开发者是否使用了交付程序。
b) 预期结果如下：
   1） 开发者提供的交付程序文档，满足 5.4.1.3.3 的要求；
   2） 能够确认开发者使用了交付程序。

6.4.1.4 测试

6.4.1.4.1 覆盖证据

该项评估应遵循以下评估方法：
a) 评估方法，评估者审查开发者提供的测试覆盖证据，确认是否满足 5.4.1.4.1 的要求；
b) 预期结果：开发者提供的测试覆盖证据，满足 5.4.1.4.1 的要求。

6.4.1.4.2 功能测试

该项评估应遵循以下评估方法：
a) 评估方法，评估者审查开发者提供的功能测试文档，确认是否满足 5.4.1.4.2 的要求；
b) 预期结果：开发者提供的功能测试文档，满足 5.4.1.4.2 的要求。

6.4.1.4.3 独立测试—抽样

该项评估应遵循以下评估方法：
a) 评估方法如下：
   1） 评估者执行测试文档中的测试样本，以验证开发者的测试结果是否正确；
   2） 评估者测试产品安全功能的一个子集，以确认产品安全功能是否按照规定运行。
b) 预期结果如下：
   1） 执行测试文档中的测试样本，验证了开发者的测试结果是正确的；
   2） 确认产品安全功能是按照规定运行。

6.4.1.5 脆弱性分析

该项评估应遵循以下评估方法：
a) 评估方法如下：
   1） 评估者执行公共领域的调查以标识产品的潜在脆弱性；
   2） 评估者执行独立的产品脆弱性分析去标识产品潜在的脆弱性，在分析过程中使用开发者提供的指导性文档、功能规范、产品设计和安全架构描述；
   3） 评估者基于已标识的潜在脆弱性实施穿透性测试，确认产品是否能够抵抗具有基本攻击潜力的攻击者的攻击。
b) 预期结果如下：
   1） 开发者提供了适合测试的产品，并提供执行脆弱性分析的相关资源；

2） 通过脆弱性分析确认产品能够抵抗具有基本攻击潜力的攻击者的攻击。

6.4.2 增强级

6.4.2.1 开发

6.4.2.1.1 安全架构描述

该项评估应遵循以下评估方法：

a） 评估方法，评估者审查产品安全功能安全架构描述文档，确认是否满足 5.4.2.1.1 的要求；

b） 预期结果：产品安全功能安全架构描述文档符合 5.4.2.1.1 的要求。

6.4.2.1.2 完备的功能规范

该项评估应遵循以下评估方法：

a） 评估方法，评估者审查开发者提供的功能规范文档，确认是否满足 5.4.2.1.2 的要求；

b） 预期结果：开发者提供了功能规范文档，并且文档符合 5.4.2.1.2 的要求。

6.4.2.1.3 基础模块设计

该项评估应遵循以下评估方法：

a） 评估方法如下：

1） 评估者审查开发者提供的产品设计文档，确认是否满足 5.4.2.1.3 中对设计文档的要求；

2） 评估者审查映射关系说明，确认是否满足 5.4.2.1.3 中对映射关系的要求；

3） 评估者确认设计是否所有安全功能要求的正确且完备的实例。

b） 预期结果如下：

1） 开发者提供的产品设计文档，满足 5.4.2.1.3 中对设计文档的要求；

2） 映射关系说明满足 5.4.2.1.3 中对映射关系的要求；

3） 能够确认设计是所有安全功能要求的正确且完备的实例。

6.4.2.1.4 安全功能实现表示

该项评估应遵循以下评估方法：

a） 评估方法如下：

1） 评估者审查开发者提供的实现表示，确认是否满足 5.4.2.1.4 中对实现表示文档的要求；

2） 评估者审查映射关系说明，确认是否满足 5.4.2.1.4 中对映射关系的要求。

b） 预期结果如下：

1） 开发者提供的实现表示，满足 5.4.2.1.4 中对实现表示文档的要求；

2） 映射关系说明满足 5.4.2.1.4 中对映射关系的要求。

6.4.2.2 指导性文档

6.4.2.2.1 准备程序

该项评估应遵循以下评估方法：

a） 评估方法如下：

1） 评估者审查开发者提供的准备程序，确认是否满足 5.4.2.2.1 的要求；

2） 评估者运用准备程序确认产品运行是否能被安全的准备。

b） 预期结果如下：

1） 开发者提供的准备程序，满足 5.4.2.2.1 的要求；
2） 运用准备程序能够做好产品安全运行的准备。

6.4.2.2.2 操作用户指南

该项评估应遵循以下评估方法：
a） 评估方法，评估者审查开发者提供的操作用户指南，确认是否满足 5.4.2.2.2 的要求；
b） 预期结果：开发者提供的操作用户指南，满足 5.4.2.2.2 的要求。

6.4.2.3 生命周期支持

6.4.2.3.1 配置管理系统的使用

该项评估应遵循以下评估方法：
a） 评估方法如下：
1） 评估者审查确认开发者是否使用了配置管理系统；
2） 评估者审查开发者提供的配置管理文档，确认是否满足 5.4.2.3.1 的要求。
b） 预期结果如下：
1） 能够确认开发者使用了配置管理系统；
2） 开发者提供的配置管理文档，满足 5.4.2.3.1 的要求。

6.4.2.3.2 部分产品配置管理覆盖

该项评估应遵循以下评估方法：
a） 评估方法，评估者审查开发者提供的产品配置项列表，确认是否满足 5.4.2.3.2 的要求；
b） 预期结果：开发者提供的产品配置项列表，满足 5.4.2.3.2 的要求。

6.4.2.3.3 生产支持和接受程序及其自动化

该项评估应遵循以下评估方法：
a） 评估方法如下：
1） 评估者审查确认开发者是否使用了配置管理系统；
2） 评估者审查开发者提供的配置管理文档，确认是否满足 5.4.2.3.3 的要求；
b） 预期结果如下：
1） 能够确认开发者使用了配置管理系统；
2） 开发者提供的配置管理文档，满足 5.4.2.3.3 的要求。

6.4.2.3.4 问题跟踪配置管理覆盖

该项评估应遵循以下评估方法：
a） 评估方法，评估者审查开发者提供的产品配置项列表，确认是否满足 5.4.2.3.4 的要求；
b） 预期结果：开发者提供的产品配置项列表，满足 5.4.2.3.4 的要求。

6.4.2.3.5 交付程序

该项评估应遵循以下评估方法：
a） 评估方法如下：
1） 评估者审查开发者提供的交付程序文档，确认是否满足 5.4.2.3.5 的要求；
2） 评估者审查确认开发者是否使用了交付程序。

b) 预期结果如下：

1） 开发者提供的交付程序文档，满足 5.4.2.3.5 的要求；

2） 能够确认开发者使用了交付程序。

6.4.2.3.6 安全措施标识

该项评估应遵循以下评估方法：

a) **评估方法如下：**

1） 评估者审查开发者提供的开发安全文档，确认是否满足 5.4.2.3.6 的要求；

2） 评估者审查确认开发者是否使用了文档中描述的安全措施。

b) **预期结果如下：**

1） 开发者提供的开发安全文档，满足 5.4.2.3.6 的要求；

2） 能够确认开发者使用了文档中描述的安全措施。

6.4.2.3.7 开发者定义的生命周期模型

该项评估应遵循以下评估方法：

a) **评估方法如下：**

1） 评估者审查开发者提供的生命周期定义文档，确认是否满足 5.4.2.3.7 的要求；

2） 评估者审查确认开发者是否使用了文档中描述的生命周期模型为产品的开发和维护提供必要的控制。

b) **预期结果如下：**

1） 开发者提供的生命周期定义文档，满足 5.4.2.3.7 的要求；

2） 能够确认开发者使用了文档中描述的生命周期模型为产品的开发和维护提供必要的控制。

6.4.2.3.8 明确定义的开发工具

该项评估应遵循以下评估方法：

a) **评估方法，评估者审查开发者所提供的开发工具文档是否明确定义了用于开发产品的工具，是否无歧义地定义所有语句和实现用到的所有协定与命令，以及所有实现依赖选项的含义；**

b) **预期结果：开发者所提供的开发工具文档明确定义了用于开发产品的工具，并且无歧义地定义所有语句和实现用到的所有协定与命令，以及所有实现依赖选项的含义。**

6.4.2.4 测试

6.4.2.4.1 覆盖分析

该项评估应遵循以下评估方法：

a) **评估方法，评估者审查开发者提供的测试覆盖分析，确认是否满足 5.4.2.4.1 的要求；**

b) 预期结果：开发者提供的测试覆盖分析，满足 5.4.2.4.1 的要求。

6.4.2.4.2 测试：安全执行模块

该项评估应遵循以下评估方法：

a) **评估方法，评估者审查开发者提供的测试深度分析，确认是否满足 5.4.2.4.2 的要求；**

b) **预期结果：开发者提供的测试深度分析，满足 5.4.2.4.2 的要求。**

6.4.2.4.3 功能测试

该项评估应遵循以下评估方法：

a) 评估方法，评估者审查开发者提供的功能测试文档，确认是否满足 5.4.2.4.3 的要求；

b) 预期结果：开发者提供的功能测试文档，满足 5.4.2.4.3 的要求。

6.4.2.4.4 独立测试—抽样

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者执行测试文档中的测试样本，以验证开发者的测试结果是否正确；

2） 评估者测试产品安全功能的一个子集，以确认产品安全功能是否按照规定运行；

b) 预期结果如下：

1） 执行测试文档中的测试样本，验证了开发者的测试结果是正确的；

2） 确认产品安全功能是按照规定运行。

6.4.2.5 关注点脆弱性分析

该项评估应遵循以下评估方法：

a) 评估方法如下：

1） 评估者执行公共领域的调查以标识产品的潜在脆弱性；

2） 评估者执行独立的产品脆弱性分析去标识产品潜在的脆弱性，在分析过程中使用开发者提供的指导性文档、功能规范、产品设计、安全架构描述和实现表示；

3） 评估者基于已标识的潜在脆弱性实施穿透性测试，确认产品是否能够抵抗具有增强型基本攻击潜力的攻击者的攻击。

b) 预期结果如下：

1） 开发者提供了适合测试的产品，并提供执行关注点脆弱性分析的相关资源；

2） 通过脆弱性分析确认产品能够抵抗具有增强型基本攻击潜力的攻击者的攻击。

6.5 性能测试

6.5.1 测试环境与工具

网络病毒监控系统典型功能测试环境与工具参见附录B中B.2。

6.5.2 增强级

6.5.2.1 负载量

该项测试遵循以下测试方法：

a) 测试方法：

1) 配置网络病毒监控系统只开启病毒检测功能；

2) 配置性能测试仪发送背景流量，进行负载量测试；

3) 配置网络病毒监控系统开启所有安全功能；

4) 配置性能测试仪发送背景流量，进行负载量测试。

b) 预期结果：

1) 网络病毒监控系统的负载量指标应达到 5.5.1.1 中规定的最低要求。

附 录 A

（资料性附录）

网络病毒监控系统运行环境与模式

A.1 运行环境概述

网络病毒监控系统以旁路方式接入网络，能够实时监测网络环境中的病毒疫情发展趋势；全面检测各种网络病毒的扫描、传输、攻击等行为；精确定位病毒的来源；评估病毒产生的网络压力状况；并准确提供病毒类别、病毒名称等信息；形成网络病毒的全局视图。

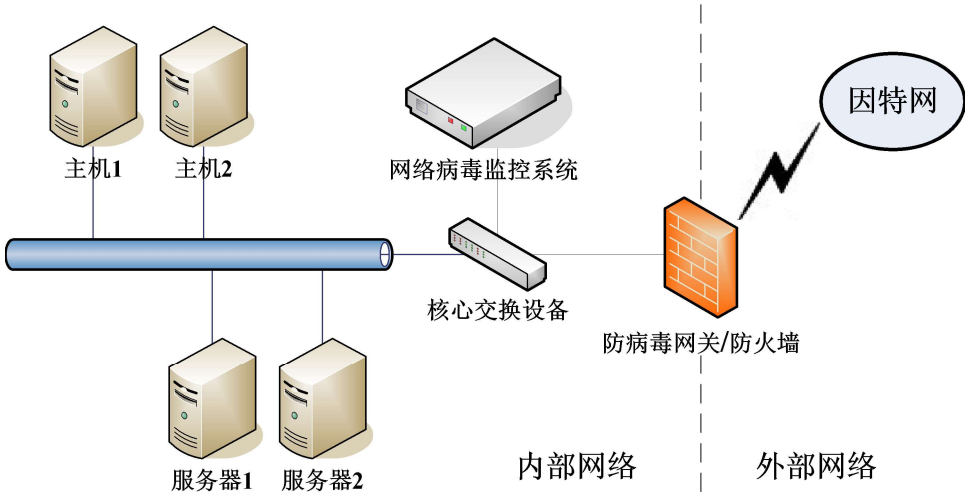

图 A.1 网络病毒监控系统典型运行环境

A.2 工作模式

网络病毒监控系统的常见工作模式是以旁路方式接入网络，不需要改变原有网络的拓扑结构，用户将不必重新设定和修改路由，无须配置网络地址，只要将网络病毒监控系统直接安装到内网镜像流量监控接口即可使用。

附 录 B

（资料性附录）

网络病毒监控系统测试环境与工具

B.1 功能测试

功能测试环境示意图可参见图B.1。其中，172.16.1.x/2::x 为外部网络地址，192.168.0.x/1::x 为内部网络地址；

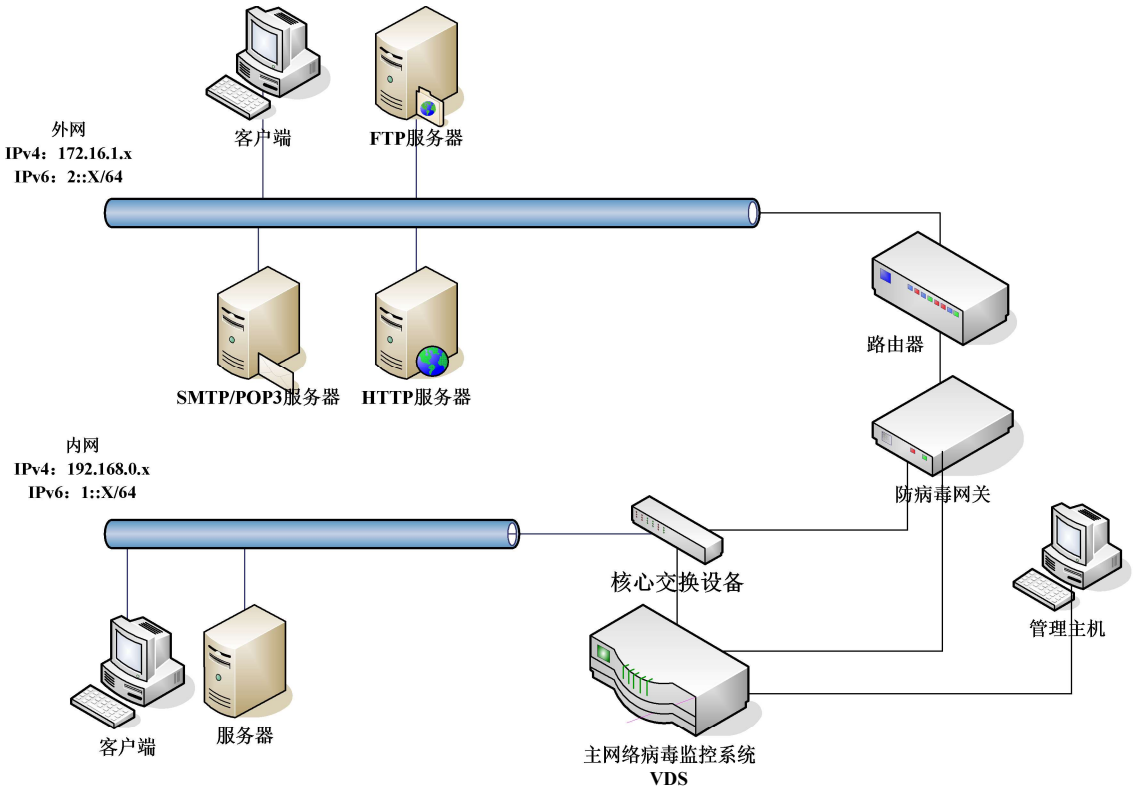

图 B.1 网络病毒监控系统功能测试环境示意图

功能测试需要的工具有：计算机病毒样本库，专用测试系统或模块，应用协议和IP包仿真器、虚拟机软件等。

B.2 病毒样本库

B.2.1 病毒样本基本库

至少包含文件型病毒、蠕虫、木马、宏病毒、脚本病毒等多种病毒类型的样本文件集合，样本文件数量不少于2000个。

B.2.2 流行病毒样本库

近三个月内流行度较高的病毒类型、病毒家族及其变种的样本文件集合，样本文件数量不少于1000个。

B.2.3 可执行病毒样本库

包含可执行病毒样本文件的集合，样本文件数量不少于30个。

B.2.4 恶意网页脚本样本库

包含恶意网页脚本样本文件的集合，样本文件数量不少于50个。

B.3 误报样本库

包含正常的操作系统文件、应用程序文件、数据文件等的文件集合，样本文件不少于1000个。

B.4 性能测试

使用专用的性能测试仪器产生测试所需的网络流量，使用分光器或交换机将网络流量进行复制或镜像，将网络病毒监控系统直接连接到网络数据镜像接口，进行测试，如图4所示。性能测试工具主要是专用性能测试设备和病毒样本库。

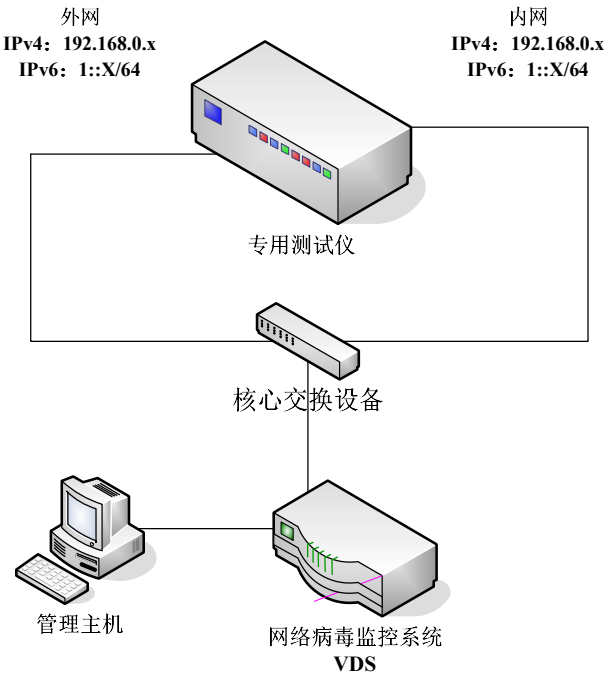

图 B.2 网络病毒监控系统性能测试环境示意图

参 考 文 献

1. 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
2. GA 243-2000 计算机病毒防治产品评级准则
3. GB/T 35277-2017 信息安全技术 防病毒网关安全技术要求和测试评价方法