ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T XXXXX—20XX

信息安全技术
APT安全监测产品安全技术要求和测试评价方法

Information security technology - Security technical requirements and testing and evaluation approaches for Advanced Persistent Threat Monitoring products

（试行）

XXXX－XX－XX 发布　　XXXX－XX－XX 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。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：国家计算机病毒应急处理中心、国家网络与信息安全信息通报中心、公安部计算机病毒防治产品检验中心、公安部计算机信息系统安全产品质量监督检验中心、公安部第一研究所、公安部第一研究所、中国科学院软件研究所、哈尔滨安天科技股份有限公司、北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司、趋势科技（中国）有限公司、南京翰海源信息技术有限公司、成都科来软件有限公司、天地融科技股份有限公司、北京赛可达信息技术有限公司、上海派博软件有限公司、杭州安恒信息技术有限公司。

本标准主要起草人：陈建民、祝国邦、张秀东、崔保红、杜振华、宋好好、张瑞、刘威、曹鹏、黄一斌、陆臻、沈亮、顾健、李毅、邹春明、顾建新、胡维娜、肖新光、应凌云、胡光俊、罗海龙、林康、张伟峰、应巧菡、许立广、王伟、杨海青、程瑞琪、赵斌、胡炯、范渊、李凯。

引　　言

本标准详细描述了与APT安全监测产品安全环境相关的假设、威胁和组织安全策略，定义了APT安全监测产品及其支撑环境的安全目的，规定了APT安全监测产品的安全功能要求、性能要求、安全保证要求及等级划分要求，通过基本原理论证安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。同时提出测试评价方法，验证APT安全监测产品是否满足相应等级规定的安全功能要求、性能要求和安全保证要求。

本标准参照了GB/T 18336-2008中规定的EAL3级安全保证要求，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本标准仅给出了APT安全监测产品应满足的安全技术要求和测试评价方法,但对APT安全监测产品的具体技术实现方式、方法等不做要求。

APT 安全监测产品安全技术要求和测试评价方法

1 范围

本标准规定了APT安全监测产品的安全功能要求、性能要求、安全保证要求及等级划分要求。

本标准适用于APT安全监测产品的设计、开发及检测。

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 18336.1－2008 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型

GB/T 18336.2－2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求

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 25069－2010 信息安全技术 术语

3 术语和定义

GB/T 18336-2008、GA 243-2000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

APT安全监测产品 Advanced Persistent Threat monitoring 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APT攻击事件的系统。

3.2

恶意软件 malware

是指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。主要包括计算机病毒、蠕虫、木马程序等破坏性程序。

3.3

恶意文档 malicious documents

是指能够利用相应文档处理程序的漏洞，执行其内嵌的恶意代码的文档文件。

3.4

APT攻击 advanced persistent threat

是指对特定目标进行的一系列高技术复杂度攻击，通常综合运用社会工程学攻击、漏洞攻击、恶意程序攻击以及采用高级隐遁技术实现对目标的组合性攻击和持续性威胁。

3.5

文件捕获 file capture

是指APT安全监测产品在检测到APT攻击时，会将可疑文件捕获存储在一个被称之为“隔离区”的受限制存储空间内，授权管理员能够对隔离区内的文件进行查阅、导出、删除等操作。

3.6

沙箱 sandbox

是指一种具有安全隔离措施的虚拟执行环境，APT安全监测产品将可疑文件在该环境中执行，并监测其文件、网络、系统操作行为，判断其危害性。

3.7

内部网络 internal network

通过网关设备隔离的可信任区域或保护区域。

3.8

外部网络 external network

通过网关设备隔离的不可信任区域或非保护区域。

3.9

负载量 peak load

APT安全监测产品在不丢包的情况下的监测能力，本标准以产品能达到的并发威胁样本的处理数量来表示。

4 缩略语

下列缩略语适用于本文件。

HTTP：超文本传输协议（HyperText Transfer Protocol）

POP3：邮局协议第3版（Post Office Protocol version 3）

FTP：文件传输协议（File Transfer Protocol）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）

HTTPS：安全超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer）

5 APT 安全监测产品描述

5.1 功能概述

APT安全监测产品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APT安全监测产品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APT安全监测产品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。

下图1是APT安全监测产品的一个典型运行环境。

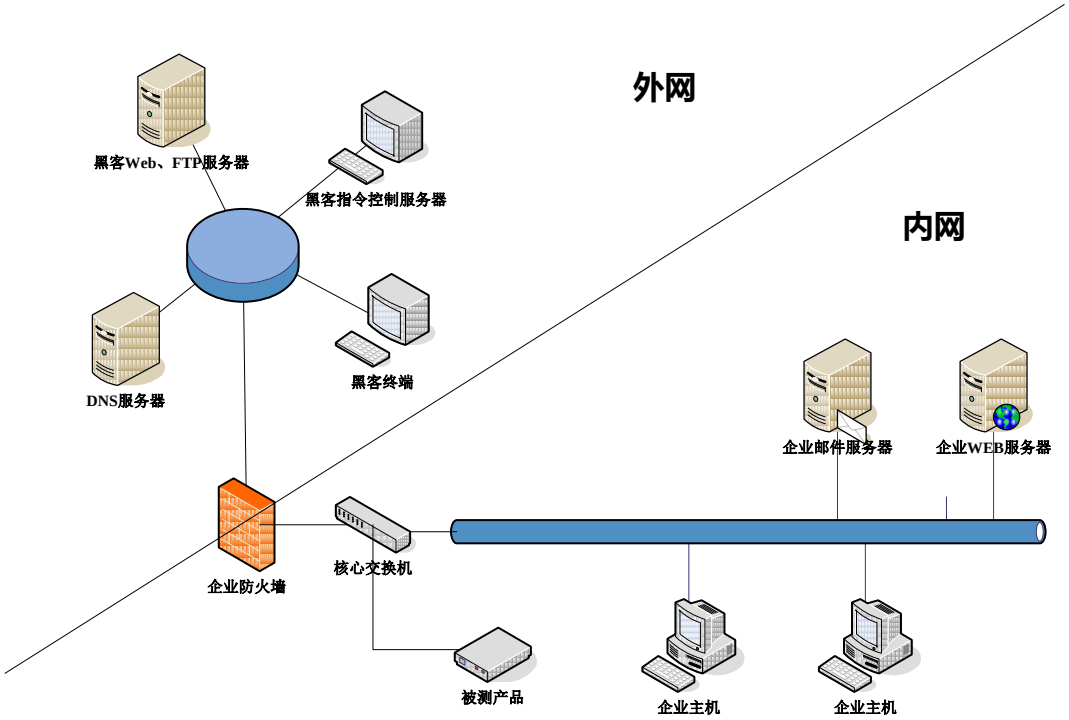

图 1 APT 安全监测产品典型运行环境

5.2 工作模式

APT安全监测产品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APT安全监测产品直接安装到内网镜像流量监控接口即可使用。

6 安全环境

6.1 假设

APT安全监测产品安全环境相关的假设如表1所示。

表1 假设

假设名称	假设描述
物理访问	产品的处理资源应限定在受控的访问设备内，以防止未授权的物理访问。所有实施产品安全策略相关的硬件和软件应受到保护，以免受非授权的物理更改
人员能力	授权管理员是无恶意的，训练有素的，并遵循管理员指南
连接性	被监控网络的通信流量必须镜像到产品
安全维护	当产品的应用环境发生变化时，应立即反映在产品的安全策略中并保持其安全功能有效

6.2 威胁

APT安全监测产品安全环境相关的威胁如表2所示。

表2　威胁

威胁名称	威胁描述
恶意漏洞扫描	恶意用户在被监控网络中，试图通过扫描获得被监控网络中的主机可能含有的漏洞信息
钓鱼攻击	恶意用户通过伪造钓鱼邮件和钓鱼网站，引诱被监测网络中的用户打开邮件或网站并访问恶意文件或 URL
地址欺骗攻击	恶意用户在被监控网络中通过 ARP 攻击或 DNS 劫持，诱使攻击目标访问恶意网络地址或文件
漏洞攻击	恶意用户在被监控网络中，利用攻击目标（包括产品本身）的操作系统漏洞/应用程序漏洞/WEB漏洞，发送攻击包，获得目标的控制权
恶意程序攻击	恶意用户在被监测网络中投放恶意程序，获得攻击目标的控制权
逃避监测	指恶意用户通过对已知攻击包或恶意程序进行修改，或恶意程序或恶意用户通过建立隐蔽信道，发送或接收指令、敏感数据，逃避监测
未知安全威胁	指恶意用户在被监测网络中利用未知攻击方式，获取攻击目标的敏感信息
组合性攻击	恶意用户在被监控网络中，通过组合运用多种攻击手段，实现对攻击目标的持续性威胁
事件记录失败	产品可能未成功记录相关安全事件；恶意用户可能通过耗尽审计数据存储空间的方法，导致事件记录的丢失或失败。从而掩盖攻击行为
非授权访问	恶意用户可能试图访问和使用产品提供的安全功能和数据
暴力认证	恶意用户可能通过反复猜测鉴别数据的方法，从而获取管理员权限
管理控制信息泄漏	恶意用户可能浏览远程授权管理员和产品之间发送的安全相关信息
设备异常	产品可能遭受断电、故障等异常情况，导致受保护的网络无法正常使用

6.3　组织安全策略

APT安全监测产品安全环境相关的组织安全策略如表3所示。

表3　组织安全策略

组织安全策略名称	组织安全策略描述
审计	为追踪所有与安全相关活动的责任，与安全相关的事件应记录、保存和审查
安全管理	产品应为授权管理员提供管理手段，使其以安全的方式进行管理

7　安全目的

7.1　产品安全目的

表4定义了产品的安全目的。这些安全目的旨在对应已标识的威胁或组织安全策略。

表4　产品安全目的

产品安全目的名称	产品安全目的描述	对应的威胁或组织安全策略
恶意程序监测	产品必须对被监测网络中传播和活动的已知和未知恶意程序进行监测，并根据策略进行响应告警	恶意程序攻击、未知安全威胁
漏洞攻击监测	产品必须对被监测网络中的已知和未知的漏洞扫描攻击行为进行监测，并根据策略进行响应告警	恶意漏洞扫描、未知安全威胁
钓鱼攻击监测	产品必须对被监测网络中的钓鱼攻击行为进行监测，并根据策略进行响应告警	钓鱼攻击
地址欺骗攻击监测	产品必须对被监测网络中的地址欺骗攻击行为进行监测，并根据策略进行响应告警	地址欺骗攻击
异常网络通信监测	产品必须对被监测网络中异常的电子邮件、Web 访问、远程控制、文件传输等网络通信行为进行监测，并根据策略进行响应报警。	未知安全威胁
逃避监测防护	指恶意用户通过对已知攻击包或恶意程序进行修改，或恶意程序或恶意用户通过建立隐蔽信道，发送或接收指令、敏感数据，逃避监测	未知安全威胁、逃避监测
隐蔽信道监测	指恶意用户通过建立隐蔽信道，在被监测网络中传输敏感信息。	未知安全威胁、逃避监测
关联分析	产品必须仲裁被监控网络内交互的信息流，通过关联分析发现潜在的组合性攻击行为，并根据策略对攻击进行告警	未知安全威胁、组合性攻击
事件记录	产品必须记录和统计病毒传播行为，记录必须具有精确的日期和时间；且产品必须提供基本的防止事件记录丢失或失败的措施	事件记录失败
身份认证	在允许用户访问产品功能之前，产品必须对用户身份进行唯一的标识和鉴别	非授权访问
鉴别失败处理	产品应具备安全机制防止恶意用户反复猜测鉴别数据，防止鉴别数据的重用	暴力认证
信息保密	如果产品允许通过相连网络对其进行远程管理，那么它必须保证远程管理信息的保密性	非授权访问、信息泄漏
用户行为可审计性	产品应对流经产品的信息流提供用户可审计性以及提供安全功能使用情况的用户可审计性	审计记录
操作系统加固	为更好地防范产品自身的漏洞，产品应确保底层支撑系统的可靠性和稳定性	漏洞攻击

失效处理	产品应具备硬件失效处理措施，保障其保护的网络能够正常使用	设备异常
安全管理	产品应向授权管理员提供以安全方式进行管理的有效手段	安全管理
审计	产品应记录自身安全相关的事件，以便追踪安全相关行为的责任，并应提供方法审查所记录的数据	审计

7.2 环境安全目的

表5定义了非技术或程序方法进行处理的安全目的。6.1部分确定的假设被包含在环境安全目的中。

表5 环境安全目的

环境安全目的名称	环境安全目的描述	对应的假设或威胁
物理访问	产品的处理资源应限定在受控的访问设备内，以防止未授权的物理访问。所有实施产品安全策略相关的硬件和软件应受到保护，以免受非授权的物理更改	物理访问
人员能力	管理员是无恶意的，训练有素的，并遵循管理员指南	人员能力
连接性	被监控网络的通信流量必须镜像到产品	连接性
安全维护	当产品的应用环境发生变化时，应立即反应在产品的安全策略中并保持其安全功能有效	安全维护

8 安全功能要求

8.1 安全监测能力

8.1.1 数据收集

产品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APT攻击检测和分析。至少应包括：

a) 常用电子邮件协议（POP3/SMTP/IMAP）；
b) 常用应用协议（HTTP/FTP/WEBMAIL）；
c) 常用远程控制工具协议（MSRDP/VNC/TEAMVIEWER/PCANYWHERE/TELNET）；
d) 常用基础网络协议（DNS/ARP）；
e) 常见 VPN 协议（PPTP/L2TP/IPSec/SSL）；
f) 其它常用应用程序通讯协议。

8.1.2 流量监测

产品应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量。

8.1.3 恶意漏洞扫描行为监测

产品应对被监控网络内发生的恶意扫描行为进行报警响应。

8.1.3.1 恶意主机漏洞扫描行为监测

产品应对被监控网络内发生的以下恶意主机扫描行为进行监测：

a) IP 地址发现扫描；
b) 端口发现扫描；
c) 操作系统发现扫描；
d) 应用服务程序发现扫描。

8.1.3.2 恶意 Web 漏洞扫描行为监测

产品应对被监控网络内发生的以下恶意主机扫描行为进行检测：

a) SQL 注入漏洞扫描；
b) XSS 漏洞扫描；
c) CGI 漏洞扫描。

8.1.4 钓鱼攻击监测

产品应对被监控网络中钓鱼攻击行为进行监测，并具有相应的响应报警能力。

8.1.4.1 钓鱼邮件攻击监测

产品应对被监测网络中以下方式的钓鱼邮件进行监测：

a) 发件人实际地址与邮件中显示的地址不一致；
b) 发件人实际地址所属网络域为伪造或与 DNS 解析结果不一致；
c) 信件内容中包含有恶意 URL 链接或恶意附件；
d) 信件内容与用户自定义的关键字或内容模版匹配。

8.1.4.2 钓鱼网站攻击监测

产品应对被监测网络中以下方式的钓鱼网站进行监测：

a) 网站域名注册信息与网站信息不符；
b) 网站无备案信息或备案信息为伪造；
c) 从网站下载的文件为含有恶意内容的文件；
d) 网站内容与用户自定义的关键字或内容模版匹配。

8.1.5 地址欺骗监测

产品应对被监测网络中以下地址欺骗方式的进行检测：

a) ARP 地址欺骗；
b) DNS 污染。

8.1.6 漏洞攻击监测

产品应对被监测网络中以下漏洞攻击方式的进行检测：

8.1.6.1 操作系统漏洞攻击监测

产品应对被监测网络中针对操作系统关键组件的漏洞攻击，并根据策略进行响应报警。

8.1.6.2 应用服务器程序漏洞攻击监测

产品应对以下针对常用的应用服务器程序的漏洞攻击行为进行检测，并根据策略进行响应报警。

a) IIS、Apache 等 Web 应用服务器程序；
b) Serv-U、TFTP 等 FTP 应用服务程序漏洞；
c) 其它应用服务器程序漏洞

8.1.6.3 浏览器漏洞攻击监测

产品应对以下针对常用的浏览器程序的漏洞攻击行为进行监测，并根据策略进行响应报警。

a) Microsoft Internet Explorer；
b) Mozilla Firefox；
c) Apple Safari
d) 其它常用浏览器程序

8.1.6.4 文件格式漏洞攻击监测

产品应对被监控网络中传输的以下含有漏洞利用代码的文件格式文件进行监测，并具有相应的响应报警能力。

a) Microsoft Office
b) WPS Office
c) Adobe Reader/Acrobat/Flash Player
d) 其它常见文件格式

8.1.6.5 WEB 漏洞攻击监测

产品应对被监测网络中以下WEB应用漏洞攻击行为进行监测，并根据策略进行响应报警。

a) SQL 注入攻击；
b) XSS 攻击；
c) 其他 WEB 漏洞攻击。

8.1.7 恶意程序攻击监测

产品应对被监测网络中传播和活动的木马后门类恶意程序进行监测，并根据策略进行响应报警。

8.1.7.1 恶意程序传播监测

产品应对被监测网络中通过以下方式传输的恶意程序进行监测，并根据策略进行响应报警。

a) POP3/SMTP/IMAP；
b) HTTP 协议；
c) FTP 协议。

8.1.7.2 恶意程序行为监测

产品应对被监测网络中恶意程序的以下活动进行监测，并根据策略进行响应报警。

a) 恶意程序与控制端的反向连接行为；
b) 恶意程序回传信息行为。

8.1.8 异常网络通信行为监测

产品应对被监测网络中的以下异常网络通信行为进行监测，并根据策略进行响应报警。

8.1.8.1 异常电子邮件行为监测

产品应对以下异常电子邮件行为进行监测：

a) 异常时间对特定电子邮件账户的访问行为；
b) 异常地点对特定电子邮件账户的访问行为；
c) 邮件内容或附件中含有特定的敏感关键字。

8.1.8.2 异常 Web 访问行为监测

产品应对以下异常Web访问行为进行监测：
a) 异常时间使用特定账户对特定 Web 应用的登录访问行为；
b) 异常地点使用特定账户对特定 Web 应用的登录访问行为；
c) 对异常 Web 应用地址的访问行为；
d) 对异常 Web 应用的提交内容中含有特定的敏感内容。

8.1.8.3 异常远程控制行为监测

产品应对以下异常远程控制访问行为进行监测：
a) 异常时间对特定主机的远程登录访问行为；
b) 异常地点对特定主机的远程登录访问行为。

8.1.8.4 异常文件传输行为监测

产品应对以下异常文件传输行为进行监测：
a) 异常时间对特定文件的传输行为；
b) 异常地点对特定文件的传输行为；
c) 对特定敏感文件的传输行为。

8.1.9 逃避监测防护

8.1.9.1 漏洞攻击逃避监测防护

产品应对以下漏洞攻击逃避行为进行监测：
a) 攻击代码混淆；
b) 数据包非标准长度、分片、乱序。

8.1.9.2 恶意程序逃避监测防护

产品应对以下恶意程序逃避行为进行监测：
a) 虚拟机识别；
b) 加壳加密。

8.1.9.3 隐蔽信道逃避监测防护

产品应对以下隐蔽信道行为进行监测：
a) 非标准端口；
b) 网络层字段隐藏；
c) 应用层 HTTP URI 隐藏
d) VPN 隧道；
e) 其他加密信道。

8.1.10 未知威胁监测

产品应对被监测网络中的未知漏洞利用行为、未知木马传播和活动行为等未知安全威胁进行监测。

8.1.10.1 未知漏洞利用行为

产品应对以下未知漏洞利用行为进行监测：

a） 文档格式漏洞；

b） 浏览器漏洞；

c） 其他应用程序未知漏洞。

8.1.10.2 未知木马传播和活动行为

产品应对以下未知木马后门传播和活动行为进行监测：

a） 木马下载行为；

b） 木马与控制端的通信行为。

8.1.11 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） 产品应支持在 IPv4/IPv6 网络应用场景中安装与正常使用。

8.2 未知威胁分析能力

8.2.1 动态沙箱分析能力

产品应具有动态沙箱分析功能，对未知漏洞和未知恶意程序进行检测。

8.2.1.1 沙箱检测能力

产品的沙箱能够对未知漏洞利用代码和恶意程序的以下行为进行动态分析：

a） 进程操作行为；

b） 文件操作行为；

c） 系统配置操作行为；

d） 网络通信行为。

8.2.1.2 沙箱扩展能力

产品的沙箱应具有扩展能力，可以根据实际需要增加沙箱数量。

8.2.2 事件关联分析能力

产品应以可视化方式提供指定时间段内，被监测网络中的特定主机与其他主机之间的相关联的已知、未知威胁事件与异常网络行为。

8.3 监测策略

8.3.1 策略自定义

产品应能根据8.1 ～ 8.2中所述的各项功能设置相应的策略配置项。并能够添加、修改和删除监测策略。

8.3.2 策略初始模板

产品应具备初始的监测策略，不允许被删除，但允许用户对此策略进行修改。

8.4 响应处理

8.4.1 告警

产品应能根据监控策略对确定的高威胁事件进行告警。

8.4.2 威胁捕获

产品应能根据监控策略对威胁事件相关的文件和数据进行加密并保存在特定的存储区域内。

8.4.3 告警信息

产品应能对已知和潜在的未知威胁事件提供告警功能。告警信息应至少包括；

a） 威胁事件时间；
b） 威胁事件类型；
c） 威胁事件名称；
d） 威胁来源；
e） 威胁目标；
f） 威胁程度；
g） 威胁详细信息。

8.4.4 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。

8.4.5 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。

8.5 报表和统计

8.5.1 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。

8.5.2 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。

8.5.3 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。

8.6 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。

8.7 升级能力

产品应支持手动或自动的方式进行升级。

a） 对特征库、策略文件、沙箱以及服务程序等进行更新；

b） 支持增量升级。

8.8 协同能力

产品应支持通过syslog协议等方式读取其他安全产品的监测日志（例如与入侵检测系统、防病毒网关、防火墙等）。

8.9 标识与鉴别

8.9.1 用户标识

8.9.1.1 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。

8.9.1.2 属性初始化

产品应提供使用默认值对创建的每个管理员的属性进行初始化的能力。

8.9.1.3 唯一性标识

产品应为管理员提供唯一标识，并能将标识与该用户的所有可审计事件相关联。

8.9.2 身份鉴别

8.9.2.1 基本鉴别

产品应在执行任何与安全功能相关的操作之前鉴别用户的身份。

a） 采用一种用户身份鉴别方式；
b） 应对同一用户采用两种或两种以上组合的用户身份鉴别方式。

8.9.2.2 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。

8.9.2.3 鉴别失败处理

当对用户鉴别失败的次数达到指定次数后，产品应能终止用户的访问。

8.10 安全管理

8.10.1 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。

8.10.2 安全角色管理

产品应能对管理员角色进行区分：

a） 具有至少两种不同权限的管理员角色；
b） 根据不同的功能模块定义各种不同权限角色。

8.10.3 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。

8.10.4 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。

8.10.5 可信管理主机

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。

8.10.6 数据完整性

产品应确保用户信息、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。

8.10.7 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、拒绝服务等的安全漏洞。

8.11 审计日志

8.11.1 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） 用户登录成功和失败；

b） 对安全策略进行更改；

c） 对管理员进行增加、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） 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、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。

8.11.2 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。

8.11.3 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。

9 安全保证要求

9.1 配置管理

9.1.1 部分配置管理自动化

配置管理系统应提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。

配置管理计划应描述在配置管理系统中所使用的自动工具，并描述在配置管理系统中如何使用自动工具。

9.1.2 配置管理能力

9.1.2.1 版本号

开发者应为产品的不同版本提供唯一的标识。

9.1.2.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

1.1.1.1 配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效维护的证据。

9.1.2.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

1.1.1.2 开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

9.1.2.4 产生支持和接受程序

1.1.1.3 开发者提供的配置管理文档应包括一个接受计划，接受计划应描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

1.1.1.4 配置管理系统应支持产品的生成。

9.1.3 配置管理范围

9.1.3.1 配置管理覆盖

配置管理范围至少应包括产品实现表示、设计文档、测试文档、指导性文档、配置管理文档，从而确保它们的修改是在一个正确授权的可控方式下进行的。

1.1.1.5 配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

9.1.3.2 问题跟踪配置管理覆盖

1.1.1.6 配置管理范围应包括安全缺陷，确保安全缺陷置于配置管理系统之下。

9.2 交付与运行

9.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

9.2.2 修改检测

交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异。还应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

9.2.3 安装、生成和启动程序

1.1.1.7 开发者应提供文档说明产品的安装、生成和启动的过程。

9.3 开发

9.3.1 功能规范

9.3.1.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；
b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

9.3.1.2 充分定义的外部接口

功能规范应包括安全功能是完备地表示的合理性。

9.3.2 高层设计

9.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 表示应是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

9.3.2.2 安全加强的高层设计

1.1.1.8 开发者提供的安全加强的高层设计应满足以下要求：

a) 描述产品的功能子系统所有接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
b) 把产品分成安全策略实施和其他子系统来描述。

9.3.3 安全功能实现的子集

实现表示应当无歧义而且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。实现表示应是内在一致的。

9.3.4 描述性低层设计

开发者应提供产品安全功能的低层设计，低层设计应满足以下要求：

a） 表示应是非形式化的；
b） 是内在一致的；
c） 按模块描述安全功能；
d） 描述每个模块的用途；
e） 根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；
f） 描述每个安全策略实施功能是如何被提供的；
g） 标识安全功能模块的所有接口；
h） 标识安全功能模块的哪些接口是外部可见的；
i） 描述安全功能模块所有接口的用途和用法，适当时应提供效果、例外情况和错误消息的细节；
j） 把产品分为安全策略实施模块和其他模块来描述。

9.3.5 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间提供对应性分析。

对于产品安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

9.3.6 非形式化产品安全策略模型

开发者应提供安全策略模型，安全策略模型应满足以下要求：

a） 表示应是非形式化的；
b） 描述所有能被模型化的安全策略的规则与特征；
c） 应包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；
d） 应阐明安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，而且是完备的。

9.4 指导性文档

9.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a） 管理员可使用的管理功能和接口；
b） 怎样安全地管理产品；
c） 在安全处理环境中应被控制的功能和权限；
d） 所有对与产品的安全操作有关的用户行为的假设；
e） 所有受管理员控制的安全参数，如果可能，应指明安全值；
f） 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
g） 所有与管理员有关的 IT 环境安全要求。

9.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a） 产品的非管理员用户可使用的安全功能和接口；
b） 产品提供给用户的安全功能和接口的使用方法；
c） 用户可获取但应受安全处理环境所控制的所有功能和权限；

d） 产品安全操作中用户所应承担的职责；

e） 与用户有关的 IT 环境的所有安全要求。

9.5 生命周期支持

9.5.1 安全措施标识

开发者应提供开发安全文档。

1.1.1.9 开发安全文档应描述在产品的开发环境中，为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、人员的和其他方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

9.5.2 开发者定义的生命周期模型

1.1.1.10 开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

9.5.3 明确定义的开发工具

1.1.1.11 开发者应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实现中每个语句的含义和所有依赖于实现的选项的含义。

9.6 测试

9.6.1 测试覆盖

9.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

9.6.1.2 覆盖分析

开发者应提供测试覆盖的分析结果。

1.1.1.12 测试覆盖的分析结果应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

9.6.2 测试：高层设计

开发者应提供测试深度的分析。

1.1.1.13 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。

9.6.3 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。

9.6.4 独立测试

9.6.4.1 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。

9.6.4.2 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。

9.7 脆弱性评定

9.7.1 误用

9.7.1.1 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） 是完备的、清晰的、一致的、合理的；

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。

9.7.1.2 分析确认

开发者应提供分析文档论证指导性文档是完备的。

9.7.2 产品安全功能强度评估

1.1.1.14 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。

9.7.3 脆弱性分析

9.7.3.1 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。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。

9.7.3.2 独立的脆弱性分析

开发者应提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

9.7.3.3 中级抵抗力

开发者应提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

10 性能要求

10.1 负荷量

APT安全监测产品的负载量视不同应用场景有所不同，具体指标要求如下：

a） 不使用沙箱等动态检测方式的条件下

1） 并发量应不低于1000个/分钟；

b） 使用沙箱等动态检测方式的条件下

1） 并发量应不低于100个/分钟。

10.2 检测率

APT安全监测产品的检测率视不同应用场景有所不同，具体指标要求如下：

a） 已知安全威胁检测率不低于100%；

b） 未知安全威胁检测率不低于80%。

11 技术要求基本原理

11.1 安全功能要求基本原理

表6说明了安全功能要求的充分必要性的基本原理，即每个产品安全目的都至少有一个安全功能要求与其对应，每个安全功能要求都至少解决了一个产品安全目的，因此安全功能要求是充分和必要的。表6中的“✓”即表明对应关系。

表6　安全功能要求基本原理

产品安全目的 / 产品功能要求	恶意程序监测	漏洞攻击监测	钓鱼攻击监测	地址欺骗攻击监测	异常网络通信监测	逃避监测防护	隐蔽信道监测	关联分析	事件记录	身份认证	鉴别失败处理	信息保密	用户行为可审计性	操作系统加固	失效处理	安全管理	审计
数据收集	✓	✓	✓	✓	✓	✓	✓					✓					
流量监测	✓	✓	✓	✓	✓	✓	✓										
恶意漏洞扫描行为监测		✓															
钓鱼攻击监测			✓														
地址欺骗监测				✓													
漏洞攻击监测		✓															
恶意程序攻击监测	✓																
异常网络通信行为监测					✓							✓					
逃避监测防护						✓											
未知威胁监测	✓	✓			✓	✓	✓	✓									
动态沙箱分析能力	✓	✓															
事件关联分析能力								✓									
策略自定义	✓																
策略初始模板	✓																
告警	✓								✓								

产品安全目的 / 产品功能要求	恶意程序监测	漏洞攻击监测	钓鱼攻击监测	地址欺骗攻击监测	异常网络通信监测	逃避监测防护	隐蔽信道监测	关联分析	事件记录	身份认证	鉴别失败处理	信息保密	用户行为可审计性	操作系统加固	失效处理	安全管理	审计
告警信息																	
告警方式	✓																
事件记录				✓													
报表生成				✓													
报表导出				✓													
统计功能				✓													
故障信息告警															✓		
升级能力	✓													✓			
协同能力	✓																
属性定义										✓							
属性初始化										✓							
唯一性标识										✓							
基本鉴别										✓			✓				
鉴别数据保护										✓		✓					
鉴别失败处理													✓				
安全功能管理											✓						
安全角色管理											✓						
安全管理方式												✓					
远程保密传输												✓					
可信管理主机										✓	✓						
数据完整性														✓			
安全支撑系统														✓			
审计日志生成									✓				✓			✓	✓

产品安全目的 / 产品功能要求	恶意程序监测	漏洞攻击监测	钓鱼攻击监测	地址欺骗攻击监测	异常网络通信监测	逃避监测防护	隐蔽信道监测	关联分析	事件记录	身份认证	鉴别失败处理	信息保密	用户行为可审计性	操作系统加固	失效处理	安全管理	审计
审计日志存储									✓				✓			✓	✓
审计日志管理													✓			✓	✓

11.2 安全保证要求基本原理

安全保证要求参照了GB/T 18336-2008中的相关要求。

12 等级划分要求

12.1 概述

按照 APT 安全监测产品的安全功能要求强度，将 APT 安全监测产品安全功能要求划分成基本级和增强级；安全保证要求基本级参照了 EAL2 级安全保证要求，增强级在 EAL3 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

12.2 安全功能要求等级划分

APT 安全监测产品的安全功能要求等级划分如表 7 所示。

表7 APT 安全监测产品安全功能要求等级划分表

安全功能要求		基本级	增强级
监测能力	数据收集	8.1.1	8.1.1
	流量监测	8.1.2	8.1.2
	恶意漏洞扫描行为监测	8.1.3.1	8.1.3.2
	钓鱼攻击监测	——	8.1.4
	地址欺骗监测	8.1.5 a）	8.1.5
	漏洞攻击监测	8.1.6	8.1.6
	恶意程序攻击监测	8.1.7	8.1.7
	异常网络通信行为监测	——	8.1.8
	逃避监测防护	8.1.9	8.1.9
	未知威胁监测	8.1.10	8.1.10
未知威胁分析能力	动态沙箱分析能力	8.2.1	8.2.1
	事件关联分析能力	8.2.2	8.2.2
监控策略	策略自定义	8.3.1	8.3.1
	策略初始模板	8.3.2	8.3.2
响应处理	告警	8.4.1	8.4.1
	威胁捕获	8.4.2	8.4.2
	告警信息	8.4.3	8.4.3
	告警方式	8.4.4	8.4.4
	事件记录	8.4.5	8.4.5

安全功能要求			基本级	增强级
报表和统计	报表生成		8.5.1	8.5.1
	报表导出		8.5.2	8.5.2
	统计功能		8.5.3	8.5.3
故障信息告警			8.6	8.6
升级能力			8.7	8.7
协同联动能力			——	8.8
标识与鉴别	用户标识	属性定义	8.9.1.1	8.9.1.1
		属性初始化	8.9.1.2	8.9.1.2
		唯一性标识	8.9.1.3	8.9.1.3
	身份鉴别	基本鉴别	8.9.2.1 a）	8.9.2.1
		鉴别数据保护	8.9.2.2	8.9.2.2
		鉴别失败处理	——	8.9.2.3
安全管理	安全功能管理		8.10.1	8.10.1
	安全角色管理		——	8.10.2
	安全管理方式		8.10.3 a）～b）	8.10.3
	远程保密传输		——	8.10.4
	可信管理主机		——	8.10.5
	数据完整性		——	8.10.6
	安全支撑系统		——	8.10.7
审计日志	审计日志生成		8.11.1	8.11.1
	审计日志存储		8.11.2	8.11.2
	审计日志管理		8.11.3	8.11.3

12.3 安全保证要求等级划分

APT 安全监测产品的安全保证要求等级划分如表 8 所示。

表8 APT 安全监测产品安全保证要求等级划分表

安全保证要求			基本级	增强级
配置管理	部分配置管理自动化		——	9.1.1
	配置管理能力	版本号	9.1.2.1	9.1.2.1
		配置项	9.1.2.2	9.1.2.2
		授权控制	——	9.1.2.3
		产生支持和接受程序	——	9.1.2.4

安全保证要求			基本级	增强级
	配置管理范围	配置管理覆盖	——	9.1.3.1
		问题跟踪配置管理覆盖	——	9.1.3.2
交付与运行	交付程序		9.2.1	9.2.1
	修改检测		——	9.2.2
	安装、生成和启动程序		9.2.3	9.2.3
开发	功能规范	非形式化功能规范	9.3.1.1	9.3.1.1
		充分定义的外部接口	——	9.3.1.2
	高层设计	描述性高层设计	9.3.2.1	9.3.2.1
		安全加强的高层设计	——	9.3.2.2
	安全功能实现的子集		——	9.3.3
	描述性低层设计		——	9.3.4
	非形式化对应性证实		9.3.5	9.3.5
	非形式化产品安全策略模型		——	9.3.6
指导性文档	管理员指南		9.4.1	9.4.1
	用户指南		9.4.2	9.4.2
生命周期支持	安全措施标识		——	9.5.1
	开发者定义的生命周期模型		——	9.5.2
	明确定义的开发工具		——	9.5.3
测试	测试覆盖	覆盖证据	9.6.1.1	9.6.1.1
		覆盖分析	——	9.6.1.2
	测试：高层设计		——	9.6.2
	功能测试		9.6.3	9.6.3
	独立测试	一致性	9.6.4.1	9.6.4.1
		抽样	9.6.4.2	9.6.4.2
脆弱性评定	误用	指南审查	——	9.7.1.1
		分析确认	——	9.7.1.2
	产品安全功能强度评估		9.7.2	9.7.2
	脆弱性分析	开发者脆弱性分析	9.7.3.1	9.7.3.1
		独立的脆弱性分析	——	9.7.3.2
		中级抵抗力	——	9.7.3.3

13 测评方法

13.1 总体说明

测评方法与技术要求意义对应，它给出具体的测评方法来验证APT安全监测产品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。

13.2 功能测试

13.2.1 测试环境与工具

功能测试环境示意图可参见图2。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；

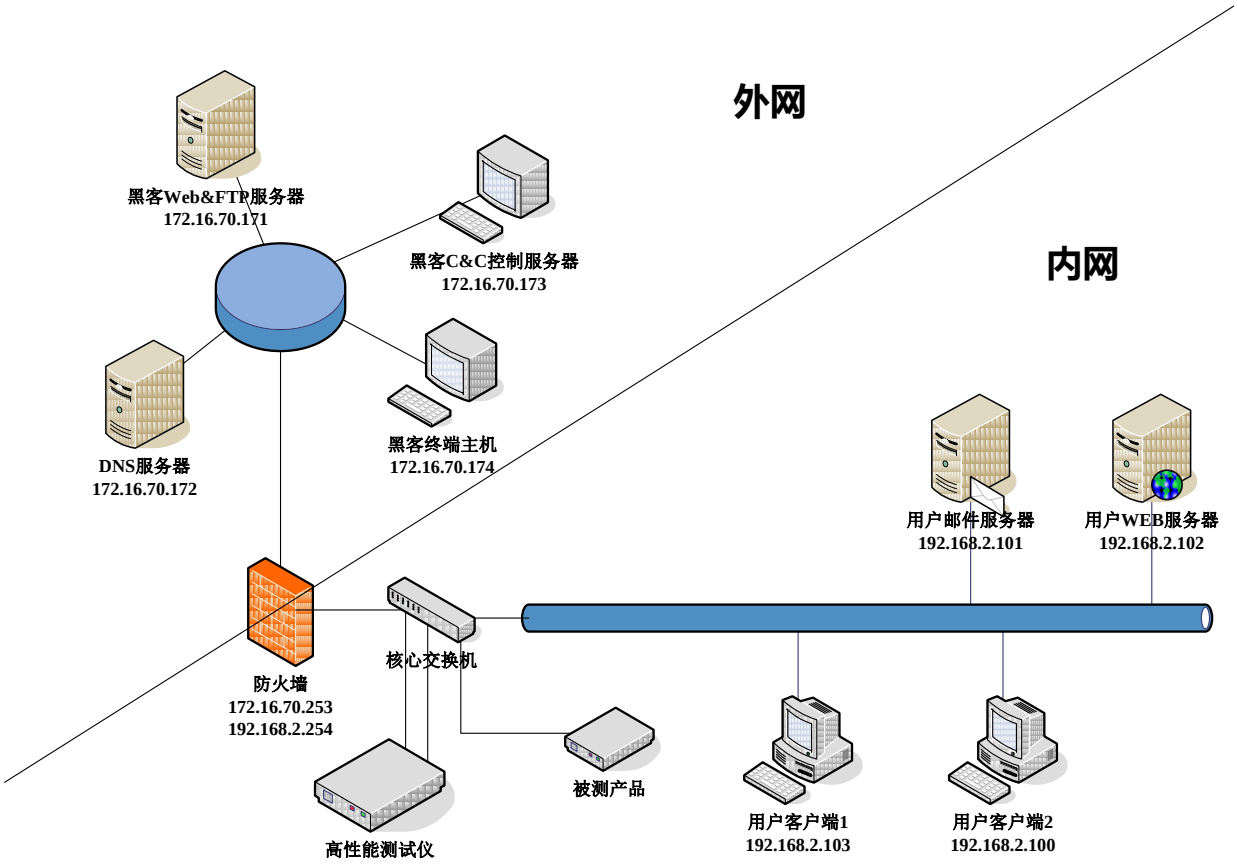

图 2 APT 安全监测产品功能测试环境示意图

功能测试需要的工具有：威胁样本库，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。

13.2.2 安全监测能力

13.2.2.1 数据收集

a) 测试方法

1) 使用测试仪或应用程序在被监测网络中产生 8.1.1 中的各类协议流量。

b) 预期结果

1) APT 安全监测产品应能够识别上述协议流量，并提供协议名称和流量信息。

13.2.2.2 流量监测

a) 测试方法
   1) 使用测试仪或应用程序在监测网络中产生 8.1.1 中的各类协议流量；
   2) 配置 APT 安全监测产品对指定协议、地址、端口的流量进行监测。
b) 预期结果
   1) APT 安全监测产品应能够识别上述协议流量，并提供协议名称、地址、端口号、报文流量和字节流量。

13.2.2.3 恶意漏洞扫描行为监测

13.2.2.3.1 恶意主机漏洞扫描行为监测

a) 测试方法
   1) 使用业内广泛使用的主机漏洞扫描软件对被监测网络中的主机进行漏洞扫描；
   2) 配置主机漏洞扫描软件的扫描内容包括 IP 地址发现、端口发现、操作系统发现和应用服务程序发现。
b) 预期结果
   1) APT 安全监测产品应能够识别上述扫描行为，并告警同时说明漏洞扫描方式。

13.2.2.3.2 恶意 Web 漏洞扫描行为监测

a) 测试方法
   1) 使用业内广泛使用的 Web 漏洞扫描软件对被监测网络中的 Web 应用进行 Web 漏洞扫描；
   2) 配置 Web 漏洞扫描软件的扫描内容包括 SQL 注入漏洞、XSS 漏洞和 CGI 漏洞。
b) 预期结果
   1) APT 安全监测产品应能够识别上述扫描行为，并告警同时说明漏洞类型。

13.2.2.4 钓鱼攻击监测

13.2.2.4.1 钓鱼邮件攻击监测

a) 测试方法
   1) 向被监测网络中发送符合 8.1.4.1 a)-c)方式的钓鱼邮件；
   2) 将若干钓鱼邮件样本提供给产品提供商，要求提供商根据钓鱼邮件样本更新特征库；
b) 预期结果
   1) APT 安全监测产品应能够识别钓鱼邮件，并告警同时说明钓鱼邮件的详细判定信息。

13.2.2.4.2 钓鱼网站攻击监测

a) 测试方法
   1) 准备符合 8.1.4.2 a)-c)中描述的钓鱼网站样本；
   2) 将若干钓鱼网站样本提供给产品提供商，要求提供商根据钓鱼网站样本更新特征库；
   3) 在被监测网络中使用客户端访问上述钓鱼网站样本。
b) 预期结果
   1) APT 安全监测产品应能够识别钓鱼网站，并告警同时说明钓鱼邮件的详细判定信息。

13.2.2.5 地址欺骗监测

a) 测试方法
   1) 使用 ARP 和 DNS 攻击工具，在被监测网络中发起攻击；
b) 预期结果
   1) APT 安全监测产品应能够检测到 ARP 地址欺骗和 DNS 污染攻击，并告警同时提供攻击源和攻击的详细信息。

13.2.2.6 漏洞攻击监测

13.2.2.6.1 操作系统漏洞攻击监测

a) 测试方法
   1) 使用漏洞攻击工具，对被监测网络中的主机操作系统发起攻击；
b) 预期结果
   1) APT 安全监测产品应能够检测漏洞攻击，并告警同时提供攻击源和攻击的详细信息。

13.2.2.6.2 应用服务器程序漏洞攻击监测

a) 测试方法
   1) 使用漏洞攻击工具，对被监测网络中的应用服务器程序发起攻击；
b) 预期结果
   1) APT 安全监测产品应能够检测漏洞攻击，并告警同时提供攻击源和攻击的详细信息。

13.2.2.6.3 浏览器漏洞攻击监测

a) 测试方法
   1) 使用漏洞攻击工具，生成含有漏洞利用代码的恶意网页；
   2) 被监测网络中的客户端使用浏览器访问恶意网页；
b) 预期结果
   1) APT 安全监测产品应能够检测漏洞攻击，并告警同时提供攻击源和攻击的详细信息。

13.2.2.6.4 文件格式漏洞攻击监测

a) 测试方法
   1) 使用漏洞攻击工具，生成含有漏洞利用代码的恶意文档；
   2) 在被监测网络中传输恶意文档；
b) 预期结果
   1) APT 安全监测产品应能够检测漏洞攻击，并告警同时提供攻击源和攻击的详细信息。

13.2.2.6.5 WEB 漏洞攻击监测

a) 测试方法
   1) 在被监测网络中构建含有漏洞的 WEB 应用程序。
   2) 使用漏洞攻击工具，向被监测网络中的 WEB 应用程序发起 SQL 注入、XSS 等漏洞攻击；
b) 预期结果
   1) APT 安全监测产品应能够检测漏洞攻击，并告警同时提供攻击源和攻击的详细信息。

13.2.2.7 恶意程序攻击监测

13.2.2.7.1 恶意程序传播监测

a) 测试方法

1) 在被监测网络中利用 8.1.7.1 a)-c)中的各种协议传输恶意程序样本；

b) 预期结果

1) APT 安全监测产品应能够检测恶意程序，并告警同时提供攻击源和恶意程序的详细信息。

13.2.2.7.2 恶意程序行为监测

a) 测试方法

1) 在被监测网络中的客户端中激活运行木马等恶意程序；
2) 使用外网的木马控制服务器向内网中的木马发送指令，查看被控客户端的各种信息；
3) 木马将客户端中的敏感文件回传到控制服务器。

b) 预期结果

1) APT 安全监测产品应能够检测恶意程序与控制服务器之间的信息传输行为，并告警同时提供攻击源和攻击的详细信息。

13.2.2.8 异常网络通信行为监测

13.2.2.8.1 异常电子邮件行为监测

a) 测试方法

1) 配置 APT 安全监测产品的异常电子邮件监测策略，包括指定电子邮件账户、异常时间、异常地点和敏感关键字等条件；
2) 在被监测网络中进行违反监测策略的电子邮件行为；

b) 预期结果

1) APT 安全监测产品应能够依照监测策略检测到异常电子邮件行为，并告警同时提供违反的策略等详细信息。

13.2.2.8.2 异常 Web 访问行为监测

a) 测试方法

1) 配置 APT 安全监测产品的异常 Web 访问行为监测策略，包括指定 Web 应用、指定账户、异常时间、异常地点和敏感关键字等条件；
2) 在被监测网络中进行违反监测策略的 Web 访问行为；

b) 预期结果

1) APT 安全监测产品应能够依照监测策略检测到异常 Web 访问行为，并告警同时提供违反的策略等详细信息。

13.2.2.8.3 异常远程控制行为监测

a) 测试方法

1) 配置 APT 安全监测产品的异常远程控制行为监测策略，包括指定主机、异常时间、异常地点等条件；
2) 在被监测网络中进行违反监测策略的远程控制行为；

b) 预期结果

1) APT 安全监测产品应能够依照监测策略检测到异常远程控制行为，并告警同时提供违反的策略等详细信息。

13.2.2.8.4 异常文件传输行为监测

a) 测试方法
   1) 配置 APT 安全监测产品的异常远程控制行为监测策略，包括指定文件、异常时间、异常地点等条件；
   2) 在被监测网络中进行违反监测策略的远程控制行为；
b) 预期结果
   1) APT 安全监测产品应能够依照监测策略检测到异文件传输行为，并告警同时提供违反的策略等详细信息。

13.2.2.9 逃避监测防护

13.2.2.9.1 漏洞攻击逃避监测防护

a) 测试方法
   1) 配置漏洞攻击工具，增加代码混淆，调整数据包长度、分片大小和发送顺序；
   2) 向被监测网络中向特定主机发起漏洞攻击。
b) 预期结果
   1) APT 安全监测产品应能够依照监测策略检测到漏洞攻击行为，并告警同时提供攻击源和攻击详细信息。

13.2.2.9.2 恶意程序逃避监测防护

a) 测试方法
   1) 将已知恶意程序加带有反虚拟机功能的壳；
   2) 向被监测网络中的客户端发送加壳后恶意程序。
b) 预期结果
   1) APT 安全监测产品应能够检测到恶意程序，并告警同时提供恶意程序来源和恶意程序详细信息。

13.2.2.9.3 隐蔽信道逃避监测防护

a) 测试方法
   1) 在外网配置端口为 80 的 FTP 服务器，在内网访问此 FTP 服务器，传输违反监测策略的文件；
   2) 在被监测网络与外网之间构造网络层字段隐藏方式的隐蔽信道；
   3) 在被监测网络与外网之间构造应用层 HTTP URI 隐藏方式的隐蔽信道
   4) 在被监测网络与外网之间构造 VPN 方式的隐蔽信道；
   5) 在被监测网络与外网之间构造 SSL 加密的隐蔽信道。
b) 预期结果
   1) APT 安全监测产品应能够依照监测策略检测到隐蔽信道，并告警同时提供隐蔽信道详细信息。

13.2.2.10 未知威胁监测

13.2.2.10.1 未知漏洞利用行为

a) 测试方法

1） 从外网向被监测网络发送未知漏洞攻击包，漏洞类型包括 8.1.10.1 a)-c)；

b） 预期结果

1） APT 安全监测产品应能够检测到未知漏洞攻击，并告警同时提供攻击来源和攻击详细信息。

13.2.2.10.2 未知木马传播和活动行为

a） 测试方法

1） 从外网向被监测网络发送未知木马恶意程序；

2） 在被监测网络中的客户端上激活木马恶意程序；

3） 在外网的木马控制主机上向被控端发送指令，获取被控端的敏感信息。

b） 预期结果

1） APT 安全监测产品应能够检测到未知恶意程序，并告警同时提供恶意程序来源和恶意程序详细信息。

13.2.2.11 多种类型网络应用场景支持

a） 测试方法

1） 在 IPv6 环境下进行 13.2 和 13.4 的所有测评内容

b） 预期结果

1） APT 安全监测产品应能够正常检测到威胁事件，并提供准确的攻击源和目的地址信息。

13.2.3 未知威胁分析能力

13.2.3.1 动态沙箱分析能力

13.2.3.1.1 沙箱检测能力

a） 测试方法

1） 开启 APT 安全监测产品的沙箱检测功能；

2） 在被监测网络中发送能够触发沙箱检测功能的威胁样本；

3） 查看监测结果。

b） 预期结果

1） APT 安全监测产品应能够通过沙箱对威胁样本进行检测，并提供 8.2.1.1 a)-d)中描述的各类行为监测信息。

13.2.3.1.2 沙箱扩展能力

a） 测试方法

1） 要求厂家通过增加单独的沙箱服务器增加沙箱数量；

b） 预期结果

1） APT 安全监测产品应能够增加单独的沙箱服务器，并能够正常对威胁样本进行检测。

13.2.3.2 事件关联分析能力

a） 测试方法

1） 查看产品是否可以以可视化方式提供指定时间段内，被监测网络中的特定主机与其他主机之间的相关联的已知、未知威胁事件与异常网络行为。

b） 预期结果

1） APT 安全监测产品应能够提供相应的信息。

13.2.4 监测策略

13.2.4.1 策略自定义

a） 测试方法

1） 根据 8.1～8.11 中的所有功能要求，配置相应策略；

b） 预期结果

1） APT 安全监测产品能够根据自定义的策略完成相应的检测和告警。

13.2.4.2 策略初始模版

a） 测试方法

1） 检查 APT 安全监测产品是否包含初始策略；

2） 尝试删除该初始策略；

3） 尝试修改此初始策略。

b） 预期结果

1） APT 安全监测产品应具有初始策略，该策略无法删除，但可以修改。

13.2.5 响应处理

13.2.5.1 告警

a） 测试方法

1） 查看 APT 安全监测产品是否可以依据监测策略对安全威胁事件进行告警；

b） 预期结果

1） APT 安全监测产品可以对安全威胁事件进行告警。

13.2.5.2 威胁捕获

a） 测试方法

1） 查看 APT 安全监测产品是否可以提供安全威胁事件的相关文件和数据；

b） 预期结果

1） APT 安全监测产品可以提供安全威胁事件的相关文件和数据。

13.2.5.3 告警信息

a） 测试方法

1） 查看 APT 安全监测产品是否可以提供 8.4.3 中描述的各项告警信息数据；

b） 预期结果

1） APT 安全监测产品的告警信息包含 8.4.3 中描述的各项告警信息数据。

13.2.5.4 告警方式

a） 测试方法

1） 查看 APT 安全监测产品是否采用屏幕实时提示、邮件告警、短信告警和声音告警等一种或多种方式。

b） 预期结果

1） APT 安全监测产品采用了屏幕实时提示、邮件告警、短信告警和声音告警等一种或多种方

式。

13.2.5.5 事件记录

a) 测试方法
   1) 查看 APT 安全监测产品是否对安全威胁事件及时生成事件记录，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。
b) 预期结果
   1) APT 安全监测产品对安全威胁事件及时生成事件记录，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。

13.2.6 报表和统计

13.2.6.1 报表生成

a) 测试方法
   1) 检查 APT 安全监测产品的报表生成配置；
   2) 使用 APT 安全监测产品提供的缺省报表模版生成报表；
   3) 配置 APT 安全监测产品的自定义报表模版；
   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) APT 安全监测产品具有报表生成功能；
   2) APT 安全监测产品提供缺省报表模版；
   3) APT 安全监测产品能够按缺省报表模版生成报表；
   4) APT 安全监测产品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。

13.2.6.2 报表导出

a) 测试方法
   1) 配置 APT 安全监测产品的报表导出设置，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) APT 安全监测产品具有报表导出功能，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) APT 安全监测产品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) APT 安全监测产品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。

13.2.6.3 统计功能

a) 测试方法
   1) 检查 APT 安全监测产品的安全事件统计功能；

2） 配置统计条件为基于 HTTP 协议的安全事件；
3） 查看统计结果是否与统计条件相符。

b） 预期结果
1） APT 安全监测产品具有安全事件统计功能；
2） APT 安全监测产品能够根据统计条件输出正确的统计结果。

13.2.7 故障信息告警

a） 测试方法
1） 人为造成 APT 安全监测产品产品的一种软件故障；
2） 人为造成 APT 安全监测产品产品的一种硬件故障。

b） 预期结果
1） 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。

13.2.8 升级能力

a） 测试方法
1） 开启 APT 安全监测产品的自动升级功能，并配置自动更新时间；
2） 通过手动方式启动 APT 安全监测产品升级；
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 APT 安全监测产品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） APT 安全监测产品能够通过自动和手动方式升级到最新版本；
2） APT 安全监测产品能够通过增量升级方式升级到最新版本。

13.2.9 协同能力

a） 测试方法
1） 以 IDS 为例，进行测试；
2） 配置 APT 安全监测产品的协同策略，并设定认证方式；
3） 通过 syslog 服务器读取 IDS 日志

b） 预期结果
1） APT 安全监测产品能够读取 IDS 的报警日志。

13.2.10 标识与鉴别

13.2.10.1 用户标识

a） 测试方法
1） 检查 APT 安全监测产品的用户管理功能，是否有分组、权限分配功能；
2） 按 APT 安全监测产品提供的默认安全属性创建一个管理员用户；
3） 检查管理员标识是否唯一。

b） 预期结果

1） APT 安全监测产品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） APT 安全监测产品可以创建一个具有默认安全属性的管理员用户；
3） 管理员标识为唯一。

13.2.10.2 身份鉴别

a） 测试方法
1） 检查 APT 安全监测产品是否有身份鉴别功能；
2） 使用 APT 安全监测产品相关安全功能前用户是否需要输入凭据；
3） 检查 APT 安全监测产品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用户的访问；
5） 检查防病毒网关是否对同一用户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） APT 安全监测产品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 APT 安全监测产品的相关安全功能；
3） APT 安全监测产品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 APT 安全监测产品；
5） APT 安全监测产品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，APT 安全监测产品能够允许用户正常登录；
7） 对于错误的凭据组合，APT 安全监测产品能够拒绝用户登录。

13.2.11 安全管理

13.2.11.1 安全功能管理

a） 测试方法
1） 使用授权管理员的合法凭据登录 APT 安全监测产品；
2） 查看、修改 APT 安全监测产品的相关安全属性；
3） 启动、关闭 APT 安全监测产品的全部或部分安全功能；
4） 新增、修改 APT 安全监测产品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 APT 安全监测产品的全部或部分安全功能；
3） 授权管理员能够新增、修改 APT 安全监测产品的病毒监控策略等各种安全策略；

13.2.11.2 安全角色管理

a） 测试方法
1） 检查 APT 安全监测产品是否有至少两种不同权限的管理员角色；
2） 检查 APT 安全监测产品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） APT 安全监测产品具有至少两种不同权限的管理员角色；

2） APT 安全监测产品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。

13.2.11.3 安全管理方式

a） 测试方法
1） 检查 APT 安全监测产品是否有 console 接口；
2） 使用 console 接口连接到 APT 安全监测产品，对 APT 安全监测产品进行管理；
3） 检查 APT 安全监测产品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 APT 安全监测产品进行管理；
5） 检查远程管理客户机与 APT 安全监测产品的通讯过程是否采用加密方式。
b） 预期结果
1） APT 安全监测产品具有 console 接口，并能够通过 console 接口对 APT 安全监测产品进行管理；
2） APT 安全监测产品具有远程管理接口,并能够通过网络远程对 APT 安全监测产品进行管理；
3） 远程管理客户机与 APT 安全监测产品之间的通讯过程采用加密方式。

13.2.11.4 远程保密传输

a） 测试方法
1） 检查 APT 安全监测产品是否由使用网络进行通讯的若干组件构成；
2） 检查 APT 安全监测产品组件间的网络通讯是否通过加密方式。
b） 预期结果
1） APT 安全监测产品各组件间的网络通讯均采用加密方式。

13.2.11.5 可信管理主机

a） 测试方法
1） 检查 APT 安全监测产品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 APT 安全监测产品的管理控制台；
3） 使用不符合限制条件的远程主机连接 APT 安全监测产品的管理控制台。
b） 预期结果
1） APT 安全监测产品能够限制远程管理主机的 IP 地址；
2） APT 安全监测产品允许符合限制条件的远程主机连接到管理控制台；
3） APT 安全监测产品拒绝不符合限制条件的远程主机连接到管理控制台。

13.2.11.6 数据完整性

a） 测试方法
1） 检查 APT 安全监测产品是否具有确保用户信息、策略信息和关键程序的完整性校验功能；
2） 使用经过破坏性修改的离线升级包对 APT 安全监测产品进行升级。
b） 预期结果
1） APT 安全监测产品具有确保用户信息、策略信息和关键程序的完整性校验功能；
2） APT 安全监测产品能够对不完整、不合法的升级包进行鉴别，取消升级过程，并提示用户。

13.2.11.7 安全支撑系统

a） 测试方法

1） 使用端口扫描器对 APT 安全监测产品进行服务端口扫描；
2） 使用 telnet、nc 等程序访问 APT 安全监测产品开放的网络端口；
3） APT 安全监测产品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 APT 安全监测产品进行漏洞检测和攻击测试。

b） 预期结果
1） APT 安全监测产品不提供多余的网络服务；
2） APT 安全监测产品不含导致产品权限丢失、拒绝服务等的安全漏洞。

13.2.12 审计日志

13.2.12.1 审计日志生成

a） 测试方法
1） 检查并开启 APT 安全监测产品的审计日志功能；
2） 分别使用正确和错误的管理员身份鉴别凭据登录 APT 安全监测产品；
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 APT 安全监测产品，直到 APT 安全监测产品终止会话连接；
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） APT 安全监测产品具有审计日志生成功能；
2） APT 安全监测产品的审计日志能够记录用户登录和失败事件；
3） APT 安全监测产品的审计日志能够记录用户对安全策略的更改事件；
4） APT 安全监测产品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） APT 安全监测产品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） APT 安全监测产品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） APT 安全监测产品的审计日志能够记录管理员的其他操作；
8） APT 安全监测产品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。

13.2.12.2 审计日志存储

a） 测试方法
1） 查看 APT 安全监测产品的审计日志；
2） 突然切断 APT 安全监测产品的电源供应；
3） 恢复 APT 安全监测产品的电源供应，查看 APT 安全监测产品的审计日志；
4） 对比断电前后的审计日志。

b） 预期结果
1） 断电重启后 APT 安全监测产品的审计日志不会丢失。

13.2.12.3 审计日志管理

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 APT 安全监测产品中的审计日志记录对比。
b) 预期结果
   1) APT 安全监测产品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 APT 安全监测产品中的审计日志记录内容相符。

13.3 安全保证测试

13.3.1 部分配置管理自动化

a) 测试方法
   1) 检查配置管理系统是否提供了一种自动方式来支持产品的生成；
   2) 检查配置管理计划中是否描述了在配置管理系统中所使用的自动工具；
   3) 检查配置管理计划中是否描述了在配置管理系统中如何使用自动工具。
b) 预期结果
   1) APT 安全监测产品的配置管理系统提供了一种自动方式来支持产品的生成；
   2) APT 安全监测产品的配置管理计划中描述了在配置管理系统中所使用的自动工具；
   3) APT 安全监测产品的配置管理计划中描述了在配置管理系统中如何使用自动工具。

13.3.2 配置管理能力

13.3.2.1 版本号

a) 测试方法
   1) 检查开发者是否为产品的不同版本提供了唯一的标识。
b) 预期结果
   1) 开发者为产品的不同版本提供了唯一的标识。

13.3.2.2 配置项

a) 测试方法
   1) 检查开发者是否使用了配置管理系统并提供了配置管理文档；
   2) 检查配置管理文档是否包括一个配置清单；
   3) 检查配置清单中是否唯一标识了组成产品的所有配置项并对配置项进行描述；
   4) 检查配置清单中是否描述了对配置项给出唯一标识的方法，并提供了所有的配置项得到有效维护的证据。
b) 预期结果
   1) 开发者使用了配置管理系统并提供了配置管理文档；
   2) 配置管理文档包括了一个配置清单；
   3) 配置清单中唯一标识了组成产品的所有配置项并对配置项进行描述；
   4) 配置清单中描述了对配置项给出唯一标识的方法，并提供了所有的配置项得到有效维护的

证据。

13.3.2.3 授权控制

a) 测试方法
   1) 检查配置管理文档是否包括一个配置管理计划；
   2) 检查配置管理计划中是否描述了如何使用配置管理系统；
   3) 检查实施的配置管理是否与配置管理计划相一致；
   4) 检查开发者是否提供了所有的配置项得到有效地维护的证据，是否保证只有经过授权才能修改配置项。
b) 预期结果
   1) 开发者使用了配置管理系统并提供了配置管理文档；
   2) 配置管理文档包括了一个配置清单；
   3) 配置清单中唯一标识了组成产品的所有配置项并对配置项进行描述；
   4) 配置清单中描述了对配置项给出唯一标识的方法，并提供了所有的配置项得到有效维护的证据。

13.3.2.4 产生支持和接受程序

a) 测试方法
   1) 检查配置管理文档中是否包括一个接受计划；
   2) 检查接受计划中是否描述了用来接受修改过的或新建的作为产品组成部分的配置项的程序；
   3) 检查配置管理系统是否支持产品的生成。
b) 预期结果
   1) 配置管理文档中包括了一个接受计划；
   2) 接受计划中描述了用来接受修改过的或新建的作为产品组成部分的配置项的程序；
   3) 配置管理系统支持产品的生成。

13.3.3 配置管理范围

13.3.3.1 配置管理覆盖

a) 测试方法
   1) 检查配置管理范围中是否包括了产品实现表示、设计文档、测试文档、指导性文档、配置管理文档；
   2) 检查上述文档的修改是否在一个正确授权的可控方式下进行；
   3) 检查配置管理文档是否能跟踪上述内容并描述了配置管理系统是如何跟踪这些配置项的。
b) 预期结果
   1) 配置管理范围中包括了产品实现表示、设计文档、测试文档、指导性文档、配置管理文档；
   2) 文档的修改是在一个正确授权的可控方式下进行的；
   3) 配置管理文档能跟踪上述内容，并且描述了配置管理系统是如何跟踪这些配置项的。

13.3.3.2 问题跟踪配置管理覆盖

a) 测试方法
   1) 检查配置管理范围中是否包括安全缺陷。

b) 预期结果

1) 配置管理范围中包括安全缺陷，确保安全缺陷置于配置管理系统之下。

13.3.4 交付程序

a) 测试方法

1) 检查开发者是否使用一定的交付程序交付产品，并将交付过程文档化；
2) 检查交付文档是否描述了在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

b) 预期结果

1) 开发者使用了一定的交付程序交付产品，并将交付过程文档化；
2) 交付文档描述了在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

13.3.5 修改检测

a) 测试方法

1) 检查交付文档是否描述了如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异；
2) 检查交付文档是否描述了如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

b) 预期结果

1) 交付文档描述了如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异；
2) 交付文档描述了如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

13.3.6 安装、生成和启动程序

a) 测试方法

1) 检查开发者是否提供了文档说明产品的安装、生成和启动的过程。

b) 预期结果

1) 开发者提供了文档说明产品的安装、生成和启动的过程。

13.3.7 功能规范

13.3.7.1 非形式化功能规范

a) 测试方法

1) 检查开发者是否提供了一个功能规范；
2) 检查功能规范是否使用了非形式化风格来描述产品安全功能及其外部接口；
3) 检查功能规范是否是内在一致的；
4) 检查功能规范是否描述了所有外部接口的用途与使用方法，是否提供了效果、例外情况和错误消息的细节；
5) 检查功能规范是否完备地表示了产品安全功能。

b) 预期结果

1) 开发者提供了一个功能规范；
2) 功能规范使用了非形式化风格来描述产品安全功能及其外部接口；

3) 功能规范是内在一致的；
4) 功能规范描述了所有外部接口的用途与使用方法，提供了效果、例外情况和错误消息的细节；
5) 功能规范完备地表示了产品安全功能。

13.3.7.2 充分定义的外部接口

a) 测试方法
1) 检查功能规范是否包括了安全功能是完备地表示的合理性。
b) 预期结果
1) 功能规范包括了安全功能是完备地表示的合理性。

13.3.8 高层设计

13.3.8.1 描述性高层设计

a) 测试方法
1) 检查开发者是否提供了产品安全功能的高层设计；
2) 检查高层设计的表示是否是非形式化的；
3) 检查高层设计是否是内在一致的；
4) 检查高层设计是否按子系统描述安全功能的结构；
5) 检查高层设计是否描述了每个安全功能子系统所提供的安全功能性；
6) 检查高层设计是否标识了安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
7) 检查高层设计是否标识了安全功能子系统的所有接口；
8) 检查高层设计是否标识了安全功能子系统的哪些接口是外部可见的。
b) 预期结果
1) 开发者提供了产品安全功能的高层设计；
2) 高层设计的表示是非形式化的；
3) 高层设计是内在一致的；
4) 高层设计按子系统描述了安全功能的结构；
5) 高层设计描述了每个安全功能子系统所提供的安全功能性；
6) 高层设计标识了安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
7) 高层设计标识了安全功能子系统的所有接口；
8) 高层设计标识了安全功能子系统的哪些接口是外部可见的。

13.3.8.2 安全加强的高层设计

a) 测试方法
1) 检查开发者是否提供了安全加强的高层设计；
2) 检查安全加强的高层设计是否描述了产品的功能子系统所有接口的用途与使用方法，是否提供了效果、例外情况和错误消息的细节；
3) 检查安全加强的高层设计是否把产品分成安全策略实施和其他子系统来描述。
b) 预期结果
1) 开发者提供了安全加强的高层设计；

2） 安全加强的高层设计描述了产品的功能子系统所有接口的用途与使用方法，提供了效果、例外情况和错误消息的细节；
3） 安全加强的高层设计把产品分成安全策略实施和其他子系统来描述。

13.3.9 安全功能实现的子集

a） 测试方法
1） 检查实现表示是否无歧义而且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；
2） 检查实现表示是否是内在一致的。
b） 预期结果
1） 实现表示无歧义而且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；
2） 实现表示是内在一致的。

13.3.10 描述性低层设计

a） 测试方法
1） 检查开发者是否提供了产品安全功能的低层设计；
2） 检查低层设计的表示是否是非形式化的；
3） 检查低层设计是否是内在一致的；
4） 检查低层设计是否按模块描述安全功能；
5） 检查低层设计是否描述了每个模块的用途；
6） 检查低层设计是否根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；
7） 检查低层设计是否描述了每个安全策略实施功能是如何被提供的；
8） 检查低层设计是否标识了安全功能模块的所有接口；
9） 检查低层设计是否标识了安全功能模块的哪些接口是外部可见的；
10） 检查低层设计是否描述了安全功能模块所有接口的用途和用法，是否提供了效果、例外情况和错误消息的细节；
11） 检查低层设计是否把产品分为安全策略实施模块和其他模块来描述。
b） 预期结果
1） 开发者提供了产品安全功能的低层设计；
2） 低层设计的表示是非形式化的；
3） 低层设计是内在一致的；
4） 低层设计按模块描述安全功能；
5） 低层设计描述了每个模块的用途；
6） 低层设计根据所提供的安全功能性和对其他模块的依赖关系两方面来定义了模块间的相互关系；
7） 低层设计描述了每个安全策略实施功能是如何被提供的；
8） 低层设计标识了安全功能模块的所有接口；
9） 低层设计标识了安全功能模块的哪些接口是外部可见的；
10） 低层设计描述了安全功能模块所有接口的用途和用法，提供了效果、例外情况和错误消息的细节；
11） 低层设计把产品分为了安全策略实施模块和其他模块来描述。

13.3.11 非形式化对应性证实

a) 测试方法
   1) 检查开发者是否提供了产品安全功能表示的所有相邻对之间的对应性分析；
   2) 检查分析是否阐明了产品安全功能所表示的每个相邻对；
   3) 较为抽象的安全功能表示的所有相关安全功能，检查开发者是否在较具体的安全功能表示中得到正确且完备地细化。
b) 预期结果
   1) 开发者提供了产品安全功能表示的所有相邻对之间的对应性分析；
   2) 分析阐明了产品安全功能所表示的每个相邻对；
   3) 较为抽象的安全功能表示的所有相关安全功能，开发者已在较具体的安全功能表示中得到正确且完备地细化。

13.3.12 非形式化产品安全策略模型

a) 测试方法
   1) 检查开发者是否提供了安全策略模型；
   2) 检查安全策略模型的表示是否是非形式化的；
   3) 检查安全策略模型是否描述了所有能被模型化的安全策略的规则与特征；
   4) 检查安全策略模型是否包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；
   5) 检查安全策略模型是否阐明了安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，而且是完备的。
b) 预期结果
   1) 开发者提供了安全策略模型；
   2) 安全策略模型的表示是非形式化的；
   3) 安全策略模型描述了所有能被模型化的安全策略的规则与特征；
   4) 安全策略模型包含了合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；
   5) 安全策略模型阐明了安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，而且是完备的。

13.3.13 管理员指南

a) 测试方法
   1) 检查开发者是否提供了管理员指南；
   2) 检查管理员指南是否与为评估而提供的其他所有文档保持一致；
   3) 检查管理员指南是否说明了管理员可使用的管理功能和接口；
   4) 检查管理员指南是否说明了怎样安全地管理产品；
   5) 检查管理员指南是否说明了在安全处理环境中应被控制的功能和权限；
   6) 检查管理员指南是否说明了所有对与产品的安全操作有关的用户行为的假设；
   7) 检查管理员指南是否说明了所有受管理员控制的安全参数，如果可能，应指明安全值；
   8) 检查管理员指南是否说明了每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
   9) 检查管理员指南是否说明了所有与管理员有关的 IT 环境安全要求。

b) 预期结果

1) 开发者提供了管理员指南；
2) 管理员指南与为评估而提供的其他所有文档保持一致；
3) 管理员指南说明了管理员可使用的管理功能和接口；
4) 管理员指南说明了怎样安全地管理产品；
5) 管理员指南说明了在安全处理环境中应被控制的功能和权限；
6) 管理员指南说明了所有对与产品的安全操作有关的用户行为的假设；
7) 管理员指南说明了所有受管理员控制的安全参数，如果可能，应指明安全值；
8) 管理员指南说明了每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
9) 管理员指南说明了所有与管理员有关的 IT 环境安全要求。

13.3.14 用户指南

a) 测试方法

1) 检查开发者是否提供了用户指南；
2) 检查用户指南是否与为评估而提供的其他所有文档保持一致；
3) 检查用户指南是否说明了产品的非管理员用户可使用的安全功能和接口；
4) 检查用户指南是否说明了产品提供给用户的安全功能和接口的使用方法；
5) 检查用户指南是否说明了用户可获取但应受安全处理环境所控制的所有功能和权限；
6) 检查用户指南是否说明了产品安全操作中用户所应承担的职责；
7) 检查用户指南是否说明了与用户有关的 IT 环境的所有安全要求。

b) 预期结果

1) 开发者提供了用户指南；
2) 用户指南与为评估而提供的其他所有文档保持一致；
3) 用户指南说明了产品的非管理员用户可使用的安全功能和接口；
4) 用户指南说明了产品提供给用户的安全功能和接口的使用方法；
5) 用户指南说明了用户可获取但应受安全处理环境所控制的所有功能和权限；
6) 用户指南说明了产品安全操作中用户所应承担的职责；
7) 用户指南说明了与用户有关的 IT 环境的所有安全要求。

13.3.15 安全措施标识

a) 测试方法

1) 检查开发者是否提供了开发安全文档；
2) 检查开发安全文档是否描述了在产品的开发环境中，为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、人员的和其他方面的安全措施；
3) 检查开发安全文档是否提供了在产品的开发和维护过程中执行安全措施的证据。

b) 预期结果

1) 开发者提供了开发安全文档；
2) 开发安全文档描述了在产品的开发环境中，为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、人员的和其他方面的安全措施；
3) 开发安全文档提供了在产品的开发和维护过程中执行安全措施的证据。

13.3.16 开发者定义的生命周期模型

a) 测试方法
   1) 检查开发者是否建立了一个生命周期模型对产品的开发和维护进行必要控制；
   2) 检查开发者是否提供了生命周期定义文档描述用于开发和维护产品的模型。
b) 预期结果
   1) 开发者建立了一个生命周期模型对产品的开发和维护进行必要控制；
   2) 开发者提供了生命周期定义文档描述用于开发和维护产品的模型。

13.3.17 明确定义的开发工具

a) 测试方法
   1) 检查开发者是否明确定义用于开发产品的工具；
   2) 检查开发者是否提供了开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。
b) 预期结果
   1) 开发者明确定义了用于开发产品的工具；
   2) 开发者提供了开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

13.3.18 测试覆盖

13.3.18.1 覆盖证据

a) 测试方法
   1) 检查开发者是否提供了测试覆盖的证据；
   2) 检查在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。
b) 预期结果
   1) 开发者提供了测试覆盖的证据；
   2) 在测试覆盖证据中，准确表明了测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

13.3.18.2 覆盖分析

a) 测试方法
   1) 检查开发者是否提供了测试覆盖的分析结果；
   2) 检查测试覆盖的分析结果是否表明了测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。
b) 预期结果
   1) 开发者提供了测试覆盖的分析结果；
   2) 测试覆盖的分析结果表明了测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

13.3.19 测试：高层设计

a) 测试方法
   1) 检查开发者是否提供了测试深度的分析；
   2) 检查深度分析是否证实了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。

b) 预期结果
   1) 开发者提供了测试深度的分析；
   2) 深度分析中证实了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。

13.3.20 功能测试

a) 测试方法
   1) 检查开发者是否测试了安全功能，将结果文档化并提供了测试文档；
   2) 检查测试文档中是否包括了测试计划，标识了要测试的安全功能，并描述了测试的目标；
   3) 检查测试文档中是否包括了测试过程，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；
   4) 检查测试文档中是否包括了预期的测试，结果应表明测试成功后的预期输出；
   5) 检查测试文档中是否包括了实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。
b) 预期结果
   1) 开发者测试了安全功能，将结果文档化并提供了测试文档；
   2) 测试文档中包括了测试计划，标识了要测试的安全功能，并描述了测试的目标；
   3) 测试文档中包括了测试过程，标识了要执行的测试，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；
   4) 测试文档中包括了预期的测试，结果表明测试成功后的预期输出；
   5) 测试文档中包括了实际测试结果，表明每个被测试的安全功能能按照规定进行运作。

13.3.21 独立测试

13.3.21.1 一致性

a) 测试方法
   1) 检查开发者是否提供了适合测试的产品；
   2) 检查开发者提供的测试集合是否与其自测产品功能时使用的测试集合相一致。
b) 预期结果
   1) 开发者提供了适合测试的产品；
   2) 开发者提供的测试集合与其自测产品功能时使用的测试集合相一致。

13.3.21.2 抽样

a) 测试方法
   1) 检查开发者是否提供了一组相当的资源，用于安全功能的抽样测试。
b) 预期结果
   1) 开发者提供了一组相当的资源，用于安全功能的抽样测试。

13.3.22 误用

13.3.22.1 指南审查

a) 测试方法
   1) 检查开发者是否提供了指导性文档；

2) 检查指导性文档是否标识了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；
3) 检查指导性文档是否是完备的、清晰的、一致的、合理的；
4) 检查指导性文档是否列出了关于预期使用环境的所有假设；
5) 检查指导性文档是否列出了对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

b) 预期结果
1) 开发者提供了指导性文档；
2) 指导性文档标识了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；
3) 指导性文档是完备的、清晰的、一致的、合理的；
4) 指导性文档列出了关于预期使用环境的所有假设；
5) 指导性文档列出了对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

13.3.22.2 分析确认

a) 测试方法
1) 检查开发者是否提供了分析文档论证指导性文档是完备的。
b) 预期结果
1) 开发者提供了分析文档论证指导性文档是完备的。

13.3.23 产品安全功能强度评估

a) 测试方法
1) 检查开发者是否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，并说明了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。
b) 预期结果
1) 开发者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，并说明了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。

13.3.24 脆弱性分析

13.3.24.1 开发者脆弱性分析

a) 测试方法
1) 检查开发者是否执行了脆弱性分析，并提供了脆弱性分析文档；
2) 检查开发者是否从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档；
3) 对被确定的脆弱性，检查开发者是否明确记录采取的措施；
4) 对每一条脆弱性，检查其是否有证据显示在使用产品的环境中，该脆弱性不能被利用。
b) 预期结果
1) 开发者执行了脆弱性分析，并提供了脆弱性分析文档；
2) 开发者从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档；
3) 对被确定的脆弱性，开发者明确记录了采取的措施；

4） 对每一条脆弱性，有证据显示在使用产品的环境中，该脆弱性不能被利用。

13.3.24.2 独立的脆弱性分析

a） 测试方法

1） 检查开发者是否提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

b） 预期结果

1） 开发者提供文档证明了经过标识脆弱性的产品可以抵御明显的穿透性攻击。

13.3.24.3 中级抵抗力

a） 测试方法

1） 检查开发者是否提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

b） 预期结果

1） 开发者提供文档证明了产品可以抵御中级强度的穿透性攻击，并提供证据说明了对脆弱性的搜索是系统化的。

13.4 性能测试

13.4.1 测试环境与工具

使用专用的性能测试仪器产生测试所需的网络流量，使用分流器或交换机将网络流量进行复制或镜像，将APT安全监测产品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。

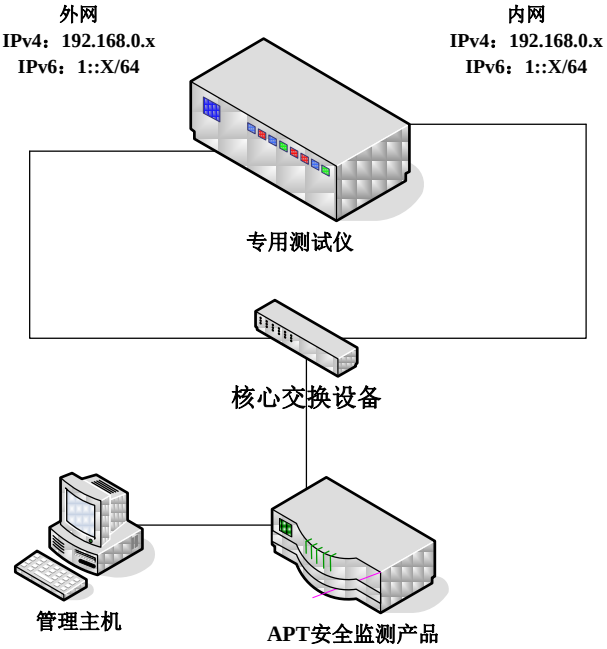

图 3 APT 安全监测产品性能测试环境示意图

13.4.2 负载量

a） 测试方法

1） 配置 APT 安全监测产品只开启静态特征检测功能；
2） 配置性能测试仪发送背景流量，进行负载量测试；
3） 配置 APT 安全监测产品开启动态检测功能；
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） APT 安全监测产品的负载量指标应达到 10.1 中规定的最低要求；

13.4.3 检测率

a） 测试方法
1） 在被监测网络中传输已知安全威胁样本；
2） 在被监测网络中传输未知安全威胁样本；

b） 预期结果
1） APT 安全监测产品的检测率指标应达到 10.2 中规定的最低要求；