

360 终端安全管理系统

测试方案

© 2024 360 企业安全集团

■ 版权申明

本文中出现的任何文字论述、文档格式、插图、照片、措施、过程等内容，除另有尤其注明外，所有版权均属 **360 企业安全集团** 所有，受到有关产权及版权法保护。任何个人、机构未经 **360 企业安全集团** 的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目 录 | Contents

1. 产品简介	1
2. 部署拓扑	1
2.1. 硬件配置规定	2
3. 天擎管理中心功能测试	3
3.1. 天擎分级部署	3
3.1.1. 天擎多级部署	3
3.2. 客户端分组管理	3
3.2.1. 客户端分组	3
3.2.2. 自动分组	3
3.2.3. 客户端分组切换	4
3.3. 客户端任务管理	4
3.3.1. 客户端天擎版本升级	4
3.3.2. 病毒库升级	4
3.3.3. 客户端任务分派管理	4
3.3.4. 手动杀毒任务	5
3.3.5. 终端查杀引擎设置	5
3.3.6. 定期杀毒任务	6
3.3.7. 消息推送	6
3.4. 客户端方略管理	6
3.4.1. 客户端软件常规安装部署方式	6
3.4.2. 终端自保护能力测试	6

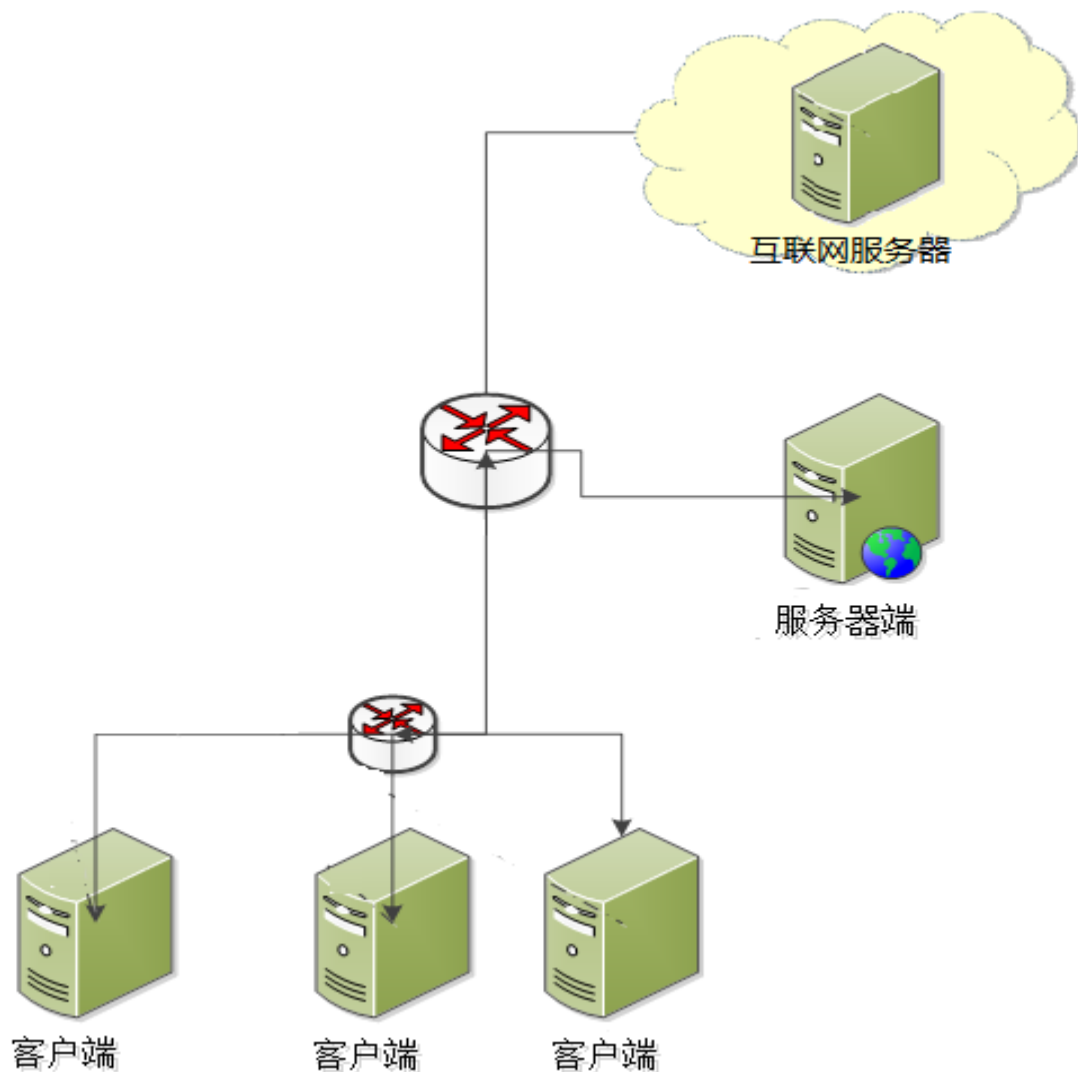
3.4.3. 客户端防退出、卸载	7
3.4.4. 离线客户端管理	7
3.4.5. 文献溯源	7
3.4.6. 黑白名单管理	8
3.4.7. 终端安全防护功能管理	8
3.4.8. 终端弹窗管理	8
3.5. 日志报表功能测试	9
3.5.1. 查杀病毒和木马日志报表	9
3.5.2. 客户端病毒状况报表	9
3.5.3. 客户端感染病毒排名榜或趋势图	9
3.5.4. 汇总多级管理架构的数据	10
3.5.5. 管理控制操作审计日志报表	10
3.6. 系统管理测试	10
3.6.1. 帐号管理及权限分派管理	10
3.6.2. 客户端与管理中心通讯间隔设置	11
3.6.3. 控制中心升级测试	11
3.6.4. 安全汇报订阅	11
3.6.5. 管理服务器备份与恢复	12
4. 天擎客户端功能验证	13
4.1. 病毒、木马查杀	13
4.2. 手动杀毒	13
4.3. 实时防护	13
4.4. 信任途径	14

4. 5. 客户端日志	14
4. 6. 客户端更新	14
5. 客户端性能测试	15
5. 1. 客户端软件常待资源消耗状况	15
5. 2. 客户端迅速扫描性能消耗状况	15
5. 3. 客户端全盘扫描性能消耗状况	15
5. 4. 客户端病毒查杀性能消耗状况	15
5. 5. 客户端病毒查杀资源回收状况	16
5. 6. 客户端文献扫描数量及时间测试	16
6. 测试总结	17

1. 产品简介

产品需专为企业顾客量身定制的内网终端安全管理软件，B/S+C/S 混合架构，支持多级管理，可以提供全网统一体检、漏洞管理、XP 加固、病毒查杀、软件管理、流量监控、资产管理等功能，并有多种组件可选，可以极大地提高内网安全管理水平。

2. 布署拓扑



客户端 布署在需要被保护的服务器或者终端，执行最终的杀毒扫描、漏洞修复等安全操作，并向安全控制中心发送对应的安全数据，可以与互联网通讯。

服务器端 采用 B/S 架构，可以随时随地的通过浏览器打开访问。重要负责设备分组管理、方略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复以及多种报表和查询等。

互联网服务器: 可以工作在终端或服务器端可以链接互联网时, 提供更新病毒库或病毒查杀服务。

2.1. 硬件配置规定

测试项目	测试天擎的管理端（总控中心）硬件规定配置
IP 地址	
CPU	Inter(R) Xeon(R) CPU E7340 @2.4GHZ 2.4GHZ
内存	8GB
硬盘	80G
操作系统	Windows Server 2023 R2 Enterprise SP1
数据库	与否支持： PostgreSQL 数据库
	☐ 支持 ☐ 不支持
备 注	

测试项目	测试天擎的管理端（一级分控中心）硬件规定配置
IP 地址	
CPU	Inter(R) Xeon(R) CPU E5-26700 @ 2.60GHZ 2.60GHZ
内存	8GB
硬盘	80G
操作系统	Windows Server 2023 R2 Enterprise SP1
数据库	与否支持： PostgreSQL 数据库
	☐ 支持 ☐ 不支持
备 注	

天擎管理中心功能测试

2.2. 天擎分级布署

2.2.1. 天擎多级布署

测试项目	天擎管理架构支持多级布署、集中管控		
布署环节	1、安装多台控制中心； 2、在二级控制中心“系统管理”-“系统工具”-“多级中心”中填入上级控制中心信息； 3、在上级控制中心“系统管理”-“多级中心”中可查看级联状况。		
测试成果	☐ 支持多级 ☐ 不支持 ☐ 只支持二级		
备 注			
测试人员		审核人员	

2.3. 客户端分组管理

2.3.1. 客户端分组

测试项目	客户端分组功能测试		
功能描述	管理员可以对树状构造通过不一样的职能、应用手工进行建立分组，并将对应的客户端加入对应分组。		
测试过程	1、进入“终端管理”页面，左侧显示“终端树”，点击设置，进入“分组管理”； 2、点击“新建分组”，选择“上级分组”，填入新建分组名，点击确认；		
测试成果	☐ 支持 ☐ 部分支持 ☐ 不支持 ☐ 未测试		
备 注			
测试人员		审核人员	

2.3.2. 自动分组

测试项目	自动分组功能测试		
功能描述	可设置按 IP、IP 段、IP 子网来实现自动分组，对于新加入的终端会自动加入到对应组		
测试过程	1、新建分组时，选择启动 IP 自动分组，填入自动分组 IP 信息； 2、新终端接入时，可按照 IP 自动分组规则加入对应分组；		
测试成果	☐ 支持 ☐ 部分支持 ☐ 不支持 ☐ 未测试		
备 注			

测试人员		审核人员	
------	--	------	--

2.3.3. 客户端分组切换

测试项目	客户端分组切换测试		
功能描述	在终端的分组信息需要变更时，可使用该功能将终端切换到其他分组，实现终端分组信息的变更，变更到其他分组后，所有的分组方略均与目前分组保持同步		
测试过程	1、进入“终端管理”页面，左侧显示“终端树”，点击设置，进入“分组管理”； 2、勾选终端，点击“转移分组”，选择需要转移到的分组；		
测试成果	☐ 支持 ☐ 部分支持 ☐ 不支持 ☐ 未测试		
备 注			
测试人员		审核人员	

2.4. 客户端任务管理

2.4.1. 客户端天擎版本升级

测试项目	客户端天擎版本升级功能测试		
功能描述	可以制定对应的计划任务来为客户端通过管控中心后台推送最新版本的天擎，以保证客户端版本的防护能力。		
测试过程	点击“终端管理”-“升级管理”，勾选终端，点击“立即升级主程序”；		
测试成果	☐ 支持 ☐ 部分支持 ☐ 不支持 ☐ 未测试		
备 注			
测试人员		审核人员	

2.4.2. 病毒库升级

测试项目	病毒库升级功能测试		
功能描述	可以针对全局、分组、某台计算机制定对应的病毒库升级计划，以保证客户端的病毒库版本更新率，提供对新病毒的查杀率。		
测试过程	点击“终端管理”-“升级管理”，勾选终端，点击“立即升级病毒库”；		
测试成果	☐ 支持 ☐ 部分支持 ☐ 不支持 ☐ 未测试		
备 注			
测试人员		审核人员	

2.4.3. 客户端任务分派管理

测试项目	客户端任务管理		
功能描述	对客户端分派任务后，可以查看已经下发的任务执行状况，并且可以撤销、删除下发的任务，同步可以看到哪些客户端已执行任务，哪些客户端未执行任务，管理员通过该功能可以掌握任务下发之后客户端的执行状况。		
测试过程	1、点击“任务管理”，查看最新任务及历史任务； 2、点击任务进度条，可以查看任务完毕状况，点击进度条，查看已完毕终端信息；		
测试成果	☐ 支持 ☐ 部分支持 ☐ 不支持 ☐ 未测试		
备 注			
测试人员		审核人员	

2.4.4. 手动杀毒任务

测试项目	手动杀毒功能测试		
功能描述	可立即对全局、分组、单点客户端下扫描任务		
测试过程	1、勾选终端，点击“迅速扫描”，提醒操作成功，在任务管理中可以找到任务记录，打开终端界面，可以看到迅速扫描界面； 2、勾选终端，点击“全盘扫描”，提醒操作成功，在任务管理中可以找到任务记录，打开终端界面，可以看到迅速扫描界面； 3、勾选终端，点击“强力查杀”，弹窗提醒选择扫描模式等信息，确认后，提醒操作完毕，并在任务管理中可以找到任务记录，打开终端界面，可以看到迅速扫描界面； 4、勾选终端，点击“文献专杀”，弹窗提醒上传专杀工具，并设置有效期，公布运行之后，在任务管理中可以找到任务记录； 5、勾选终端，点击“隔离区恢复”，选择需要回滚的隔离区文献，点击“恢复”，查看终端隔离区中，文献被移除隔离区；		
测试成果			
备 注			
测试人员		审核人员	

2.4.5. 终端查杀引擎设置

测试项目	终端查杀引擎设置		
功能描述	可对不一样分组、不一样单点终端进行查杀引擎的启动或关闭，不一样类型的终端采用不一样的引擎进行查杀；		
测试过程	1、点击“终端管理”-“病毒查杀”，进入病毒查杀管理界面； 2、针对某台终端，修改“杀毒引擎防护”，修改之后终端会与修改保持一致； 3、点击“方略中心”-“病毒查杀”-“多引擎设置”		

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。

如要下载或阅读全文，请访问：

<https://d.book118.com/948016010016006073>