清华永新统一安全网关TN-SG5000 V5.0

测试总结报告（V1.0）

(内部资料 请勿外传)

**江苏清华永新安全科技有限公司**

**版权所有 不得复制**

1 引言 5

1.1 编写目的 5

1.2 背景 5

1.3 用户群 5

1.4 定义 5

1.5 测试对象 6

1.6 测试阶段 6

2 测试概要 6

2.1 缺陷修复率 6

2.2 缺陷严重程度分布 6

2.3 缺陷类型分布 6

2.4 缺陷功能分布 7

2.5 缺陷人员分布 7

2.6 测试执行 7

2.7 测试用例 7

2.7.1 功能性 7

2.7.2 易用性 7

2.7.3 性能 8

2.7.4 可靠性 8

2.7.5 安全性 8

3 测试环境 8

3.1 软硬件环境 8

4 测试结论 9

5 测试记录 9

5.1系统管理 9

5.2包过虑规则 16

5.3网络地址转换 19

5.4带宽管理 22

5.5用户认证（Web认证） 23

5.6连接管理 24

5.7应用协议控制 25

5.8策略路由 28

5.9动态端口开放 29

5.10 IP/MAC绑定 31

5.11系统监控 32

5.12虚拟连接对 34

5.13基于域名的包过滤 35

5.14记录日志 36

5.15安全网关自身抗扫描攻击 37

5.16入侵检测 38

# 引言

## 编写目的

编写该测试总结报告主要有以下几个目的

1． 通过对测试结果的分析，得到对软件质量的评价

2． 分析测试的过程，产品，资源，信息，为以后制定测试计划提供参考

3． 评估测试测试执行和测试计划是否符合

4． 分析系统存在的缺陷，为修复和预防bug提供建议

## 背景

TN-SG5000是面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统安全网关，并具有强劲应用层处理能力的全新网络安全设备。TN-SG5000解决了传统安全设备在应用管控、应用可视化、应用内容防护等方面的巨大不足，同时开启所有功能后性能不会大幅下降。

TN-SG5000 不但可以提供基础网络安全功能，如状态检测、VPN、抗DDoS、NAT等；还实现了统一的应用安全防护，可以针对一个入侵行为中的各种技术手段进行统一的检测和防护，如应用扫描、漏洞利用、Web入侵、非法访问、蠕虫病毒、带宽滥用、恶意代码等。TN-SG5000可以为不同规模的行业用户的数据中心、广域网边界、互联网边界等场景提供更加精细、更加全面、更高性能的应用内容防护方案。

本次测试为江苏清华永新统一安全网关的系统测试。

## 用户群

主要读者：项目管理人员，项目测试经理

其他读者：项目相关人员。

## 定义

**严重bug**：出现以下缺陷，测试定义为严重bug

系统无响应，处于死机状态，需要其他人工修复系统才可复原。

点击某个菜单后出现“The page cannot be displayed”或者返回异常错误。

进行某个操作（增加、修改、删除等）后，出现“The page cannot be displayed” 或

者返回异常错误

当对必填字段进行校验时，未输入必输字段，出现“The page cannot be displayed”

或者返回异常错误

系统定义不能重复的字段输入重复数据后，出现“The page cannot be displayed”或

者返回异常错误

## 测试对象

测试版本：V5.0

## 测试阶段

系统测试。

# 测试概要

## 缺陷修复率

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Bug总数** | **关闭Bug** | **修复Bug** | **挂起Bug** | **开放Bug** | **拒绝Bug** |
| 706 | 615（87.1%） | 3(0.4%) | 60(8.5%) | 19(2.7%) | 9(1.3%) |

## 缺陷严重程度分布

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bug总数** | **严重Bug** | **较严重Bug** | **一般Bug** | **建议Bug** |
| 706 | 37（5.2%） | 87（12.3%） | 528（74.8%） | 54（7.6%） |

## 缺陷类型分布

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bug总数** | **新需求** | **设计缺陷** | **语法** | **质量保证** | **功能** | **界面** | **其它** |
| 706 | 3（0.4%） | 10（1.4%） | 1（0.14%） | 0（0%） | 531（75.6%） | 151（21.4%） | 10（1.4%） |

## 缺陷功能分布

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bug总数** | **全局控制** | **分组控制** | **内容审计** | **行为报警** | **黑白名单** | **流量分析** | **日志管理** |
| 706 | 24（3.3%） | 40（5.7%） | 156（22.1%） | 64（9%） | 13（1.9%） | 55（7.8%） | 112（15.9%） |

|  |  |  |  |
| --- | --- | --- | --- |
| **Bug总数** | **统计报表** | **系统管理** | **其它** |
| 706 | 101（14.3%） | 59（8.2%） | 82（11.6%） |

## 缺陷人员分布

|  |  |  |
| --- | --- | --- |
| **人员** | **产生Bug数** | **平均每天产生bug数** |
| 3 | 706 | 17 |

## 测试执行

此次测试严格按照项目计划和测试计划执行，按时完成了测试计划规定的测试对象的测

试。针对测试计划规定的测试策略，在测试执行中都有体现，在测试执行过程中，依据测试

计划和测试用例，对系统进行了完整的测试

## 测试用例

### 功能性

系统实现的主要功能，包括网络行为审计、内容审计、策略控制、报表统计等。

系统实现的次要功能，包括为用户权限、系统参数配置等。

需求规定的输入输出字段，以及需求规定的输入限制

### 易用性

操作按钮提示信息正确性，一致性，可理解性

限制条件提示信息正确性，一致性，可理解性

必填项标识

输入方式可理解性

中文界面下数据语言与界面语言的一致性

### 性能

各种配置的设备在对应的设计处理流量下处理数据是否丢包

界面操作响应时间、结果显示时间

封堵过滤和审计匹配逻辑处理时间

### 可靠性

7\*24周期运行的故障率

出现故障之后不影响网络通畅

磁盘空间自动维护

### 安全性

系统本身抗攻击的能力

审计日志数据防止篡改

统计报表数据防止篡改

数据传输防止窥探

# 测试环境

## 软硬件环境

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 操作系统 | CPU | 内存 | 硬盘 | 安装软件(说明版本号、Build号、补丁号) |
| AS5U2 | ITNel(R) Celeron(R) CPU 2.40GHz | 1G | 160G | rtx\_eTNerprise\_v3.0.0.1\_build060000\_single.tar.gz |
| AS5U2 | ITNel(R) Petium(R) CPU E7400 | 2G | 500G | rtx\_eTNerprise\_v3.0.0.1\_build060000\_single.tar.gz |
| AS5U2 | ITNel(R) Xeon(R) CPU E5405 | 4G | 1200G | rtx\_eTNerprise\_v3.0.0.1\_build060000\_single.tar.gz |

# 测试结论

整体功能测试通过。

# 测试记录

## 5.1系统管理

|  |  |
| --- | --- |
| 测试子项目 | **管理员三权管理分立** |
| 测试原理 | 测试是否对管理员权限进行三权分立 |
| 测试说明 | 网络安全设备的管理员权限应分为三类  **超级管理员**：只能够创建配置管理员和审计管理员，不能对设备的配置进行修改，不能查看日志信息  **配置管理员**：只能够修改安全网关配置，不能对管理员的行为进行审计，无权创建用户  **审计管理员**：只能够查看日志，审计管理员动作，不能修改安全网关配置，无权创建用户 |
| 测试步骤 | 测试的管理员权限是否按三权分立标准来设定的 |
| 预期结果 | **超级管理员**只能够创建配置管理员和审计管理员，不能对设备的配置进行修改，不能查看日志信息  **配置管理员**只能够修改安全网关配置，不能对管理员的行为进行审计，无权创建用户  **审计管理员**只能够查看日志，审计管理员动作，不能修改安全网关配置，无权创建用户 |
| 实际测试结果 | **可实现对管理员权限进行三权分立。** |
| 厂家功能界面截图 |  |

|  |  |
| --- | --- |
| 测试子项目 | **系统配置管理1** |
| 测试原理 | 考察安全网关产品是否具备灵活的配置管理功能，是否支持通过加密方式(SSH或HTTPS)进行管理以及功能模块的管理控制，是否通过集中监控来管理多台设备。 |
| 测试步骤 | 1. 支持通过Console口登录设备并进行配置管理 2. 支持通过Telnet进行配置管理 3. 支持通过SSH进行配置管理 4. 支持通过加密的HTTPS方式进行配置管理 5. 支持独立管理口 |
| 预期结果 | 支持上述各种管理方式 |
| 实际测试结果 | 支持通过Console口登录设备并进行配置管理  支持通过Telnet进行配置管理  支持通过SSH进行配置管理  支持通过加密的HTTPS方式进行配置管理  支持独立管理口 |
| 厂家功能界面截图 |  |

|  |  |
| --- | --- |
| 测试子项目 | **系统配置管理2** |
| 测试原理 | 考察安全网关产品是否具备灵活的配置管理功能，是否支持配置导出、导入，配置备份。 |
| 测试步骤 | 1. 支持配置导入导出 2. 支持手动、自动配置备份 3. 基于时间的配置自动备份 4. 支持FTP、邮件等模式的自动配置备份 |
| 预期结果 | 支持上述各种配置导入导出与备份 |
| 实际测试结果 | 系统支持配置导出、导入，实现配置备份。 |
| 厂家功能界面截图 | 点击“系统管理”-----点击“配置”，点击“备份”。 |

|  |  |
| --- | --- |
| 测试子项目 | **Web界面具备CLI终端操作** |
| 测试原理 | 考察安全网关产品是否具备灵活的CLI操作配置管理功能，是否支持通过Web方式对设备命令行下的配置，方便管理员多种配置。 |
| 测试拓扑 |  |
| 测试步骤 | 1. 登录安全网关Web管理界面； 2. 点击CLI控制台功能 |
| 预期结果 | 可在Web管理页面下，使用CLI终端对设备经行命令行配置 |
| 实际测试结果 |  |
| 厂家功能界面截图 | 点击 |

|  |  |
| --- | --- |
| 测试子项目 | **功能模块支持开启与关闭** |
| 测试原理 | 考察安全网关产品在不需要部分不能时，可根据需求关闭该模块功能，以减少对设备资源的占用。 |
| 测试拓扑 |  |
| 测试步骤 | Web管理页面操作对部分功能模块进行关闭与开启 |
| 预期结果 | 可对功能模块进行开启与关闭 |
| 实际测试结果 | 可对系统功能模块进行启动、关闭、重启启动操作。 |
| 厂家功能界面截图 | 点击“系统”----“功能控制” |

|  |  |
| --- | --- |
| 测试子项目 | **设备在线抓包** |
| 测试原理 | 考察安全网关产品在网络故障时，能够使用安全网关产品在线抓包，并可直接在管理页面查看抓包详细信息，不需要将数据包导出设备使用工具查看 |
| 测试拓扑 |  |
| 测试步骤 | Web管理页面操作抓包功能 |
| 预期结果 | 可查看设备抓包信息，包括数据包信息以及数据包详细信息 |
| 实际测试结果 | 使用安全网关产品在线抓包，并可直接在管理页面查看抓包详细信息，不需要将数据包导出设备使用工具查看。 |
| 厂家功能界面截图 | 点击“网络配置”----“数据包抓获” |

|  |  |
| --- | --- |
| 测试子项目 | **基于安全网关策略的流量统计** |
| 测试原理 | 考察安全网关产品对安全网关策略的监控，及时了解所配置的策略的正确性 |
| 测试拓扑 |  |
| 测试步骤 | Web管理界面查看安全网关策略 |
| 预期结果 | 可显示每条策略的流量统计 |
| 实际测试结果 | 可对安全网关策略的监控，可了解所配置的策略的正确性。 |
| 厂家功能界面截图 | 1. 点击“安全状态“。   2.系统显示每条策略的流量，包括上传传输及下载传输。 |

|  |  |
| --- | --- |
| * + - 1. 厂家功能界面截图 | 1．点击“对象”---“服务”。  2．系统显示所有服务类型： |

## 5.2包过虑规则

|  |  |
| --- | --- |
| 测试子项目 | **测试安全网关规则配置功能1-允许** |
| 测试拓扑 |  |
| 测试原理 | 为所有认证的用户隐藏并允许 LAN到WAN 流量 |
| 测试步骤 | 1. 为安全网关配置从lan到wan的一条允许的规则。 2. 用户从lan访问wan。 |
| 预期结果 | 内网用户可以访问外网。 |
| 实际测试结果 | 内网用户可以访问外网。 |
| 厂家功能界面截图 | 1. **配置安全网关访问规则：点击“安全网关”—“规则”。** 2. **配置规则，定义动作为“允许”。**  1. 点击确定。 |

|  |  |
| --- | --- |
| 测试子项目 | **测试安全网关规则配置功能2-拒绝** |
| 测试拓扑 |  |
| 测试原理 | 安全网关通过规则，不允许指定内部用户访问公网。 |
| 测试步骤 | 1. 为安全网关配置从lan到wan的一条拒绝的规则。 2. 用户从lan访问wan。 |
| 预期结果 | 内网用户不能访问外网。 |
| 实际测试结果 | 内网用户不能访问外网。 |
| 厂家功能界面截图 | **配置安全网关访问规则：**   1. **点击“安全网关”---“规则”：** 2. 点击“添加”，配置动作为“拒绝”。   点击确定。 |

## 5.3网络地址转换

|  |  |
| --- | --- |
| 测试子项目 | **安全网关对网络地址转换的支持** |
| 测试拓扑 |  |
| 测试原理 | 网络地址转换可以解决正式注册IP不足的问题，可以对进入的IP包进行转换，实际应用为地址映射和重定向。安全网关系统的地址转换规则分为地址映射和重定向两种。 |
| 测试步骤 | 1. 配置安全网关NAT规则PC1可正常转换访问外网地址； 2. 配置IP地址映射规则，Clinet访问安全网关外网接口IP可正常访问内网相关服务，同时内网PC1可通过安全网关外网接口映射IP地址与服务器真实地址访问相应服务； 3. 配置端口映射规则，Clinet访问安全网关外网接口IP的相应端口可正常访问内网相关服务，同时内网PC1可通过安全网关外网接口映射IP地址与服务器真实地址访问相应服务。 |
| 预期结果 | 内网PC1经NAT后可访问外网地址，同时内网PC1可通过安全网关外网接口映射IP地址与服务器真实地址访问相应服务。 |
| 实际测试结果 | 内网PC1经NAT后可访问外网地址，同时内网PC1可通过安全网关外网接口映射IP地址与服务器真实地址访问相应服务。 |
| 厂家功能界面截图 | **测试项一：配置安全网关NAT规则PC1可正常转换访问外网地址**  内网地址在192.168.1.1与192.168.1.200地址段之间的PC可访问外网。  **测试项二：配置IP地址映射规则，Clinet访问安全网关外网接口IP可正常访问内网相关服务，同时内网PC1可通过安全网关外网接口映射IP地址与服务器真实地址访问相应服务**   1. 在一台PC（连LAN口）上启用FTP服务。 2. 点击“策略配置”---“虚拟IP”，添加一条FTP服务的虚拟主机，   注：上图中“外部IP“为安全网关wan口IP地址，用户访问此地址即可访问到相应的服务；“映射IP”为内网中提供FTP服务的IP地址。   1. 在外网一台PC上，打开浏览器ftp://安全网关IP地址。   系统提示FTP登录用户名及密码。 |

## 5.4带宽管理

|  |  |
| --- | --- |
| 测试项目 | **基于安全网关规则的的带宽管理** |
| 测试原理 | 测试目的在于考察系统是否支持针对安全网关规则进行带宽管理。 |
| 网络拓扑图 |  |
| 测试步骤 | 1. 添加带宽管理策略； 2. 应用基于安全网关规则的应用带宽管理策略。 |
| 预期结果 | 应用基于安全网关规则的带宽管理策略以后，用户的上网速度被限制在限定速度之内。 |
| 实际测试结果 | 用户的外网访问速度被限制在限定速度之内。 |
| 厂家功能界面截图 | 1. 点击流量控制策略，点击“添加”。   添加一条带宽策略：  点击确认 |

## 5.5用户认证（Web认证）

|  |  |
| --- | --- |
| 测试子项目 | **安全网关提供客户端接入网络认证（Web认证）** |
| 测试拓扑 |  |
| 测试原理 | 测试目的在于考察待测系统是否具有使用WEB（无客户端）进行用户认证的功能。用户端无需安装任何认证软件 |
| 测试步骤 | 1、新建一个用户：test， 密码为test，选择好其他属性  2、增加一条认证的安全网关策略：源地址pc1，目的地址安全网关地址，服务：  3、配置一条HTTP的安全网关规则，开启身份认证选项并选择验证类型  4、Pc1访问server的http服务：通过IE浏览器打开server的http，pc1的IE界面弹出认证，输入用户名test、密码test  5、在PC1上打开一个Server网页，访问正常  6、不执行第7步骤，pc1无法访问server的http服务  7、用户成功登陆后记录用户登陆日志  8、记录在线用户流入和流出流量记录 |
| 预期结果 | 1. 通过web方式可以灵活认证 2. 通过认证后用户才能访问指定范围区域 |
| 实际测试结果 | 通过test帐号可以通过认证，认证成功后可以访问http服务 |
| 厂家功能界面截图 |  |

## 5.6连接管理

|  |  |
| --- | --- |
| 测试子项目 | **安全网关提供针对终端及服务器的新建连接数与并发连接数限制** |
| 测试拓扑 |  |
| 测试原理 | 由于网络应用的复杂会导致安全网关状态表数目资源有限和服务器连接资源有限问题变得比较严重，比如在出现蠕虫或者攻击对服务器和安全网关进行大量连接攻击时，安全网关必须具有连接限制的功能，否则将导致自身状态表满或者服务器连接资源被消耗干净。 |
| 测试步骤 | * + - 1. 1、查看是否支持连接限制的设置       2. 2、支持哪些连接限制的类型       3. 3、设置测试是否支持并发连接和新建连接   4、连接是否支持查询/阻断/统计/排序 |
| 预期结果 | 1. 支持限制主机、限制服务、保护主机、保护服务四种类型 2. 支持限制并发和新建连接，且类型可以支持tcp、udp 3. 可以指定网段、打个IP地址的并发和新建连接 4. 支持共享和独享的方式 5. 支持查询/阻断/统计/排序 |
| 实际测试结果 | 支持限制主机、限制服务、保护主机、保护服务四种类型  支持限制并发和新建连接，且类型可以支持tcp、udp  可以指定网段、打个IP地址的并发和新建连接  支持共享和独享的方式  支持查询/阻断/统计/排序 |
| 厂家功能界面截图 |  |

## 5.7应用协议控制

本测试项目测试安全网关系统预定义所能支持的服务类型，支持的类型多少影响了网络设备同其它系统的兼容性，重点考察对目前业务网络系统及将来需要扩展的业务协议支持能力。

|  |  |  |  |
| --- | --- | --- | --- |
| * + - 1. **预定义协议** | | | * + - 1. **测试结果** |
| * + - 1. AH | | | □是/□否 |
| * + - 1. AOL | | | □是/□否 |
| * + - 1. BGP | | | □是/□否 |
| * + - 1. DHCP | | | □是/□否 |
| * + - 1. DNS | | | □是/□否 |
| * + - 1. ESP | | | □是/□否 |
| * + - 1. FINGER | | | □是/□否 |
| * + - 1. FTP | | | □是/□否 |
| * + - 1. GOPHER | | | □是/□否 |
| * + - 1. GRE | | | □是/□否 |
| * + - 1. H323 | | | □是/□否 |
| * + - 1. HTTP | | | □是/□否 |
| * + - 1. HTTPS | | | □是/□否 |
| * + - 1. ICMP | | | □是/□否 |
| * + - 1. IGMP | | | □是/□否 |
| * + - 1. IKE | | | □是/□否 |
| * + - 1. IMAP | | | □是/□否 |
| * + - 1. INFO\_ADDRESS | | | □是/□否 |
| * + - 1. INFO\_REQUEST | | | □是/□否 |
| * + - 1. IPv6\_Over\_IPv4 | | | □是/□否 |
| * + - 1. IRC | | | □是/□否 |
| * + - 1. L2TP | | | □是/□否 |
| * + - 1. LDAP | | | □是/□否 |
| * + - 1. NFS | | | □是/□否 |
| * + - 1. NTNP | | | □是/□否 |
| * + - 1. TNP | | | □是/□否 |
| * + - 1. OSPF | | | □是/□否 |
| * + - 1. PC-Anywhere | | | □是/□否 |
| * + - 1. PING | | | □是/□否 |
| * + - 1. POP3 | | | □是/□否 |
| * + - 1. PPTP | | | □是/□否 |
| * + - 1. QUAKE | | | □是/□否 |
| * + - 1. RAUDIO | | | □是/□否 |
| * + - 1. RIP | | | □是/□否 |
| * + - 1. RLOGIN | | | □是/□否 |
| * + - 1. SAMBA | | | □是/□否 |
| * + - 1. SIP | | | □是/□否 |
| * + - 1. SIP-MSNmessenger | | | □是/□否 |
| * + - 1. SMTP | | | □是/□否 |
| * + - 1. SSH | | | □是/□否 |
| * + - 1. SNMP | | | □是/□否 |
| * + - 1. SYSLOG | | | □是/□否 |
| * + - 1. TALK | | | □是/□否 |
| * + - 1. TCP | | | □是/□否 |
| * + - 1. TELNET | | | □是/□否 |
| * + - 1. TFTP | | | □是/□否 |
| * + - 1. TIMESTAMP | | | □是/□否 |
| * + - 1. UDP | | | □是/□否 |
| * + - 1. UUCP | | | □是/□否 |
| * + - 1. VDOLIVE | | | □是/□否 |
| * + - 1. WAIS | | | □是/□否 |
| * + - 1. WINFRAME | | | □是/□否 |
| * + - 1. X-WINDOWS | | | □是/□否 |
| * + - 1. 动态协议支持 | * + - 1. FTP | | □是/□否 |
| * + - 1. TFTP | | □是/□否 |
| * + - 1. PPTP | | □是/□否 |
| * + - 1. H.323 | | □是/□否 |
| * + - 1. SIP | | □是/□否 |
| * + - 1. 对未提供的协议是否可以自定义 | | | □是/□否 |
| * + - 1. **协议自定义支持** | | | * + - 1. **测试结果** |
| * + - 1. 支持协议自定义 | | * + - 1. TCP任意 | □是/□否 |
| * + - 1. UDP任意 | □是/□否 |
| * + - 1. IP协议任意 | □是/□否 |
| * + - 1. ICMP任意 | □是/□否 |
| * + - 1. 预期结果 | | 可以显示以上所有类型，以及可以根据用户自定义 | |
| * + - 1. 实际测试结果 | | 显示以上所有类型，可以根据用户自定义 | |

## 5.8策略路由

|  |  |
| --- | --- |
| 测试项目 | **安全网关提供防火墙能够根据源/目的 IP 地址等参数来设置路由策略，且策略路由有效。** |
| 测试拓扑 |  |
| 测试原理 | 策略路由是尽管存在当前最优的路由，但是针对某些特别的主机（或应用、协议）不使用当前路由表中的转发路径而单独使用别的转发路径。在数据包转发的时候发生作用、不改变路由表中任何内容。 |
| 测试步骤 | 1、准备多条出口线路  2、定义路由策略 |
| 预期结果 | 1. 能够按指定接口选择路由路径 |
| 实际测试结果 | 支持策略路由让用户从指定出口转发数据 |
| 厂家功能界面截图 |  |

## 5.9动态端口开放

|  |  |
| --- | --- |
| 测试项目 | 测试主动模式和被动模式的 FTP，具备动态开放端口功能 |
| 测试拓扑 |  |
| 测试原理 | FTP数据连接的协商分为两种模式，一种是主动模式，另一种是被动模式。  主动模式的特点是，在客户端和服务器端要进行文件传递时，首先是客户端使用一个报文告诉服务器端，它将用某个IP地址的某个端口作为数据连接，也就是通常说的PORT命令。服务器端收到这个报文后，回应一个同意的ACK报文，然后服务器端会主动用自己的IP地址加上端口20来发 送一个SYN报文到客户端通过PORT命令告诉它的那个IP地址和端口，和客户端建立起一个数据连接。  被动模式的特点是，在客户端和服务器端要进行文件传递时，首先是服务器端通过一个报文告诉客户端，它将用那一个IP地址的那一个端口作为数据连接，也就是PASV命令。客户端收到这个报文之后，回应一个同意的ACK报文。然后客户端会用自己的IP地址，然后任选一个能够使用的端口和服务器端告诉它的那个IP地址和端口相连接，建立数据连接。 |
| 测试步骤 | 1. 开启ftp session-helper 2. 开启允许访问ftp服务器策略 |
| 预期结果 | 主动模式和被动模式的 FTP，客户端都可以正常连接 |
| 实际测试结果 | 主动模式和被动模式的 FTP，客户端都可以正常连接 |
| 厂家功能界面截图 |  |

## 5.10 IP/MAC绑定

|  |  |
| --- | --- |
| 测试项目 | 手工绑定 IP/MAC 地址，能够检测 IP 地址盗用，拦截盗用 IP 地址的主机经过防火墙的各种访问。 |
| 测试拓扑 |  |
| 测试原理 | 1. 测试IP和MAC绑定的基本功能，以及在MAC地址匹配而IP地址不匹配和IP地址匹而MAC地址不匹配得两种IP欺骗的情况下防火墙的处理能力 2. 在制定IP和MAC绑定规则时，可以只绑定一个区域当中的某几个主机的地址，绝大多数主机可能不需要绑定，此时，我们还可以指定防火墙对那些没指定的主机的绑定过滤规则。这个用例主要用来测试防火墙对绑定规则之外的主机的访问的处理能力 |
| 测试步骤 | 1. 通过测试仪器模拟仿真两个终端之间进行数据交互，同时发送对应的IP和MAC的数据包，防火墙检测数据包中IP地址和MAC地址匹配情况，进行流量动作；然后通过在测试以上进行IP和MAC对应关系的修改，观察并记录此时防火墙的行为 |
| 预期结果 | 符合规则的通过，不符合规则的IP不能够访问 |
| 实际测试结果 | 符合规则的通过，不符合规则的IP不能够访问 |
| 厂家功能界面截图 |  |

## 5.11系统监控

|  |  |  |
| --- | --- | --- |
| 测试子项目 | **测试安全网关能否提供非常的系统监控能力** | |
| 测试原理 | 提供丰富的监控手段对安全管理员对网络运行情况与设备运行情况提供丰富的可视化分析提供依据 | |
| 测试步骤 | 1. 查看相关的监控选项； 2. 能看到相关的实际运行情况； | |
| **测试项目** | | **测试结果** |
| 系统监控内容 | 基于IP连接统计 | □是/□否 |
| 基于IP流量统计 | □是/□否 |
| HA状态 | □是/□否 |
| 日志信息 | □是/□否 |
| 资源状态：CPU、内存、当前并发连接 | □是/□否 |
| 网络接口状态与流量 | □是/□否 |
| 网络接口接收发送数据包 | □是/□否 |
| VPN隧道（包括PPTP、L2TP） | □是/□否 |
| DHCP用户信息 | □是/□否 |
| 在线用户 | □是/□否 |
| 在线管理员 | □是/□否 |
| ARP表 | □是/□否 |
| 透明桥转发表 | □是/□否 |
| IP地址冲突检测 | □是/□否 |
| 安全网关路由表监控 | □是/□否 |
| 安全网关配置WEB查询 | □是/□否 |
| 预期结果 | 支持以上各种类型 | |
| 实际测试结果 | 支持以上各种类型 | |
| 厂家功能界面截图 |  | |

## 5.12虚拟连接对

|  |  |
| --- | --- |
| 测试子项目 | 测试目的在于考察安全网关网口联动功能，如果联动中的一个端口失去物理连接，那么另一个端口将down状态，然后链路数据转向另一组，保证网络正常通信。 |
| 测试拓扑 |  |
| 测试原理 | 在实际应用中，为了保证网络的稳定性与冗余性，经常要求安全网关的一组接口保持同样的状态。也就是说，只要这组中的某个接口断线后，也要相关的接口全部达到断线的效果，这样其他外围设备通过端口状态来判断链路是否正常，通过切换链路来达到网络畅通，保证业务能够正常运行。 |
| 测试步骤 | * + - 1. 1、设置安全网关:将port1和port2为一个网口联动组；将port3和port4为一个网口联动组       2. 2、设置安全网关规则：       3. 3、允许pc1访问server       4. 4、安全网关设置路由负载功能       5. 5、路由器1、2通过metric值得不同来选择路由，且开启端口6、状态检测功能：即路由器发现与其连接的端口为down的状态， 那么重新选择新的路由方式       6. 7、模拟链路故障，拔掉port1（或者port3），检查port2（或者port4）是否为down的状态       7. 模拟故障后，检察路由器2是否选择的新的路由   故障发生时，pc是否仍然可以访问server |
| 预期结果 | * + - 1. 当port1或者port3出现故障时，port2或者port4联动功能立即停止工作。那么路由器2立即重新选择新的路由。减少由于port2或port4仍然正常，而导致路由不可达的丢包现象 |
| 实际测试结果 |  |
| 厂家功能界面截图 | 1. **点击“网络”-“接口”** 2. **点击“添加 虚拟连接对”；** |

## 5.13基于域名的包过滤

|  |  |
| --- | --- |
| 测试子项目 | * + - 1. 测试目的在于考察安全网关基于域名过滤的功能 |
| 测试拓扑 |  |
| 测试原理 | 互联网中域名与IP地址是一一相对应，是通过DNS服务器解析来实现IP地址的访问。然而，互联网的发展迅速也存在了不同地点、不同时间、不同运营商而导致同一域名对应的IP地址不相同，因此安全网关此功能为了解决这一问题而提出的。 |
| 测试步骤 | * + - 1. 1、如拓扑所示连接设置：安全网关连接互联网       2. 2、安全网关设置禁止内网访问外网的安全规则：目的地址是某互联网域名服务器，例如[www.baidu.com](http://www.sina.com.cn)   3、内网pc通过IE浏览器打开域名地址，试图连接该互联网网址 |
| 预期结果 | * + - 1. 内网pc无法访问该域名服务器的任何服务 |
| 实际测试结果 | 无法访问baidu域名 |
| 厂家功能界面截图 |  |

## 5.14记录日志

|  |  |
| --- | --- |
| 测试子项目 | **安全网关提供记录用户访问过的URL详细日志** |
| 测试拓扑 |  |
| 测试原理 | * + - 1. 记录用户访问过的URL，通过安全规则来控制某个地址是否启用该功能，提供管理员针对IP对象访问互联网的详细日志记录。 |
| 测试步骤 | 1. 开启URL日志设备功能 2. 在相应的安全规则中引用URL日志 3. 查看相关日志信息，内容包括：get、put、post、head、delete、trace信息 4. 以上日志记录不仅支持常用80端口，是否还支持手动自定义 |
| 预期结果 | 1. 支持记录访问网页所get、put、post、head、delete、trace信息 2. 除常见80端口外，还可以手动设置其他端口 |
| 实际测试结果 |  |
| 厂家功能界面截图 |  |

## 5.15安全网关自身抗扫描攻击

|  |  |
| --- | --- |
| 测试子项目 | **测试安全网关自身抗扫描攻击** |
| 测试拓扑 |  |
| 测试原理 | 安全网关自身应该没有对外的漏洞，保证自身的安全性 |
| 测试步骤 | 1. 提供相关的扫描工具 2. 对安全网关IP进行扫描攻击与PING、Syn\_flood攻击 3. 同时查看安全网关运行状态是否正常 |
| 预期结果 | 1. 扫面工具扫面安全网关无任何信息 2. 可以抗syn\_flood、ping等厂家攻击 3. 安全网关在受到攻击时运行一切稳定 |
| 实际测试结果 | 扫面工具扫面安全网关无任何信息  可以抗syn\_flood、ping等厂家攻击  安全网关在受到攻击时运行一切稳定 |
| 厂家功能界面截图 |  |

## 5.16入侵检测

|  |  |
| --- | --- |
| 测试子项目 | **入侵检测** |
| 测试原理 | 测试目的在于考察增加了入侵检测以后是否能够阻断外部对内部的攻击，并呈现相关的告警信息 |
| 网络拓扑图 |  |
| 测试步骤 | 1. 添加入侵检测策略； 2. 在“安全网关”---“规则”添加相应规则。 |
| 预期结果 | 能够阻断相关攻击，并在日志查看页面看到相关告警信息。 |
| 实际测试结果 | 1、能够阻断相关攻击，“日志及报表”--“日志查看器”--“入侵检测”页面看到相关告警信息，某些告警信息不能体现在“日志及报表”--“日志查看器”--“入侵检测”页面，需要到“日志及报表”--“日志查看器”--“安全网关设置”中查看相关被底层阻断的告警。  2、“日志查看器”只能查看当天的日志，其他时间的日志需要到报表中进行查询  3、报表查询，查询目标显示为攻击非入侵检测，报表显示的信息较少不能反映出具体的告警信息 |
| 厂家功能界面截图 | 1. 点击入侵检测 2. 点击“添加”。   添加一条入侵检测策略。  选择后点击“确定”完成策略建立。   1. 点击“安全网关”--“规则”--“添加”。 2. 新建一个“规则”选择相关区域如：LAN--DMZ，子网主机可以根据需要来进行相关添加，“动作”选择“允许”，“入侵检测”处选择之前建立的入侵检测策略。   5．操作完成以后点击“确定”保存。 |

附表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 检测项目（GB/T 20281-2015信息安全技术 防火墙安全技术要求和测试评分方法（基本级）） | | | | 测试用例 |
| 安  全  功  能  检  测 | 网络层 控制 | 包过滤 | | 5.2 |
| NAT | | 5.3 |
| 状态检测 | | 5.2 |
| 策略路由 | | 5.8 |
| 动态开放端口 | | 5.9 |
| IP/MAC 地址绑定 | | 5.10 |
| 流量会话管理 | 流量统计 | 5.11 |
| 连接数控制 | 5.6 |
| 应用层协议控制 | | | 5.7 |
| 安全运维管理 | 运维管理 | | 5.1 |
| 安全审计 | | 5.14 |
| 管理口独立 | | 5.1 |
| 安全支撑系统 | | 5.15 |
| 异常处理机制 | | 5.15 |