

ICS 33.040

M 15



# 中华人民共和国通信行业标准

YD/T 2874-2015

---

## LTE 无线网络安全网关测试方法

Testing methods for security gateway in LTE network

2015-07-14 发布

2015-10-01 实施

---

中华人民共和国工业和信息化部 发布



# 目 次

前 言	II
1 范围	1
2 术语和定义	1
3 缩略语	1
4 测试基本要求	2
4.1 测试环境	2
4.2 测量仪表	2
4.3 供电电源	2
5 功能测试	2
5.1 测试拓扑图	2
5.2 PKI功能测试	3
5.3 IPSec VPN功能测试	6
5.4 攻击防范功能测试	9
5.5 路由支持功能测试	11
5.6 IPv6功能测试	18
5.7 地址转换功能测试	19
5.8 可靠性功能测试	22
5.9 配置管理功能测试	24
5.10 日志告警测试	24
6 性能测试	28
6.1 IPSec并发连接数与新建连接数测试数测试	28
6.2 IPSec吞吐量和时延测试	29
参考文献	30





## 前 言

本标准是LTE无线网络安全网关系列标准之一。该系列标准的名称如下：

- a) 《LTE无线网络安全网关技术要求》；
- b) YD/T 2874 《LTE无线网络安全网关测试方法》。

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：北京交通大学、华为技术有限公司、中国联合网络通信集团有限公司。

本标准主要起草人：吴 昊、黄 敏、张 东、王光全、夏俊杰、马 铮、白晓媛。



# LTE 无线网络安全网关测试方法

## 1 范围

本标准规定了LTE无线网络环境中安全网关设备或系统的接口测试、功能测试、协议测试、网管测试、可靠性测试和常规测试。

本标准适用于对LTE无线网络环境中的安全网关设备的测试。

## 2 术语和定义

下列术语和定义适用于本文件。

### 2.1

**安全网关 Security Gateway**

部署在EPC及E-UTRAN之间的设备，负责对传输的信息进行加密、过滤等功能。

### 2.2

**包过滤 Packet Filtering**

通过检查包头内容来控制访问的过程。

### 2.3

**拒绝服务攻击 Denial of Service**

利用协议缺陷，发送大量伪造的连接请求，从而使得被攻击方资源耗尽的攻击方式。

## 3 缩略语

下列缩略语适用于本文件。

AH	Authentication Head	认证报头协议
Bps	Bit per second	每秒比特率
CA	Certification Authority	数字证书认证中心
CPE	Customer Premise Equipment	用户端设备
CRL	Certificate Revocation List	证书吊销列表
DoS	Denial of Service	拒绝服务攻击
DUT	Device Under Test	被测设备
EPC	Evolved Packet Core	演进核心网
ESP	Encapsulating Security Payload	封装安全载荷
FTP	File Transfer Protocol	文件传输协议
GTP	GPRS Tunneling Protocol	GPRS隧道协议
IKE	Internet Key Exchange	因特网密钥交换协议
IPSEC	IP Security Protocol	因特网安全协议
MME	Mobility Management Entity	移动性管理实体

PKI	Public Key Infrastructure	公钥基础设施
SCEP	Simple Certificate Enrollment Protocol	简单证书注册协议
SCTP	Stream Control Transmission Protocol	流控传输协议
SeGW	Secure Gateway	安全网关
S-GW	Serving Gateway	服务网关
SNMP	Simple Network Management Protocol	简单网络管理协议
VPN	Virtual Private Network	虚拟专用网

## 4 测试基本要求

### 4.1 测试环境

如果被测设备对测试环境有特殊要求，应在规定的测试环境下测试。如无特殊测试环境要求，则应在以下环境下测试。

#### 4.1.1 温度

被测SeGW应在 $23\pm 5^{\circ}\text{C}$ 的温度下进行测试。

#### 4.1.2 湿度

被测SeGW应在30%~75%RH的相对湿度下进行测试。

#### 4.1.3 大气压

被测设备应在86~106kPa的大气压下进行测试。

#### 4.1.4 电压

直流供电设备：对使用-48V的被测设备，应选择-54V $\pm 1\text{V}$ 直流进行测试。对使用其他直流电压等级的被测设备，应选择额定输入电压进行测试，直流电压允许偏差 $\pm 2\%$ 。

交流供电设备：应在交流220V $\pm 1\%$ ，50Hz $\pm 1\%$ 条件下测试。

### 4.2 测量仪表

对测量仪表要求如下：

- a)  $\geq 80\text{kHz}$ 的输入带宽；
- b) 交流电压表准确度不低于 $\pm 1\%$ ；直流电压表准确度不低于 $\pm 0.5\%$ ；
- c) 峰值因数 $\geq 5$ 。

### 4.3 供电电源

- 1) 直流电源：电压波动率 $\leq 2\%$ ，纹波电压 $\leq 3\%$ 。
- 2) 交流电源：电压和频率波动率 $\leq 1\%$ ，2~39次总谐波失真 $\leq 5\%$ 。

## 5 功能测试

### 5.1 测试拓扑图

在CEI和PE之间布置安全网关SeGW，并通过CEI与Switch相连。CA服务器分别连接eNodeB和SeGW。测试结构拓扑如图1所示。

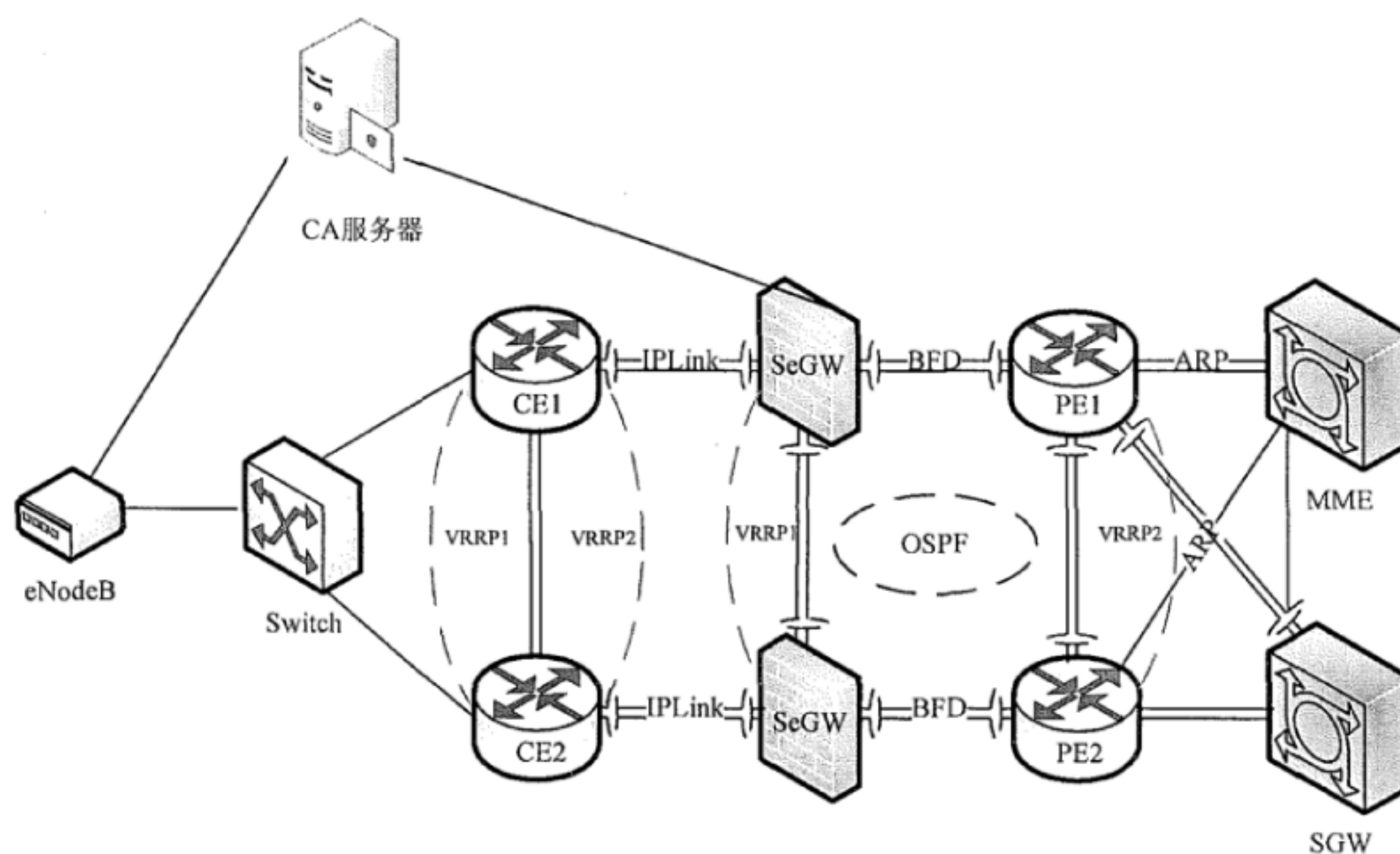


图1 测试拓扑

## 5.2 PKI 功能测试

### 5.2.1 证书申请、更新功能测试

测试项目	证书申请、更新功能测试
测试内容	能够成功的进行证书的申请、更新等功能
测试准备	1.SeGW工作正常; 2.SeGw开启CRL验证; 3.SeGW与CA、CRL服务器可正常通信, 并且CA、CRL服务器支持SCEP协议
测试步骤	1.首先配置PKI域; 2.使用SCEP协议在线申请CA/RA证书; 3.安装CA/RA证书, 安装本地证书; 4.手动下载CRL; 5.验证证书有效性
预期结果	1.命令查看证书配置文件是否存在; 2.验证步骤5中证书是否有效

## 5.2.2 PKI 删除证书和吊销列表功能测试

测试项目	验证删除证书和吊销列表功能
测试内容	SeGW 删除证书和吊销列表功能可用
测试准备	1.SeGW 工作正常; 2.SeGw 开启 CRL 验证; 3.SeGW 与 CA、CRL 服务器可正常通信, 并且 CA、CRL 服务器支持 SCEP 协议
测试步骤	1. 将证书和 CRL 加载到 SeGW; 2. 在 SeGW 上执行 PKI 删除证书和证书吊销列表的命令; 3. 在 SeGW 上执行 more ca_config.ini 来检查是否已经删除
预期结果	1. 加载证书和 CRL 成功; 2. 删除命令下发成功; 3. 证书已经被删除

## 5.2.3 交叉证书管理功能测试

测试项目	交叉证书管理功能测试
测试内容	能够成功的进行交叉证书管理功能
测试准备	1.SeGW工作正常; 2.SeGw开启CRL验证; 3.SeGW与CA、CRL服务器可正常通信, 并且CA、CRL服务器支持SCEP协议
测试步骤	1.首先配置PKI域; 2. 使用SCEP协议在线申请CA/RA证书; 3.安装CA/RA证书; 4.安装经过本地CA认证的交叉CA公钥证书; 5.安装交叉CA认证的本地证书; 6.验证证书有效性
预期结果	1. 命令查看证书配置文件是否存在; 2. 验证步骤6中证书是否有效。



## 5.2.4 PKI 使用证书属性过滤功能测试

测试项目	验证证书属性过滤功能
测试内容	证书控制策略可以验证协商中证书的有效性
测试准备	1.SeGW 工作正常; 2.SeGw 开启 CRL 验证; 3.SeGW 与 CA、CRL 服务器可正常通信, 并且 CA、CRL 服务器支持 SCEP 协议
测试步骤	1.IPSEC 基本功能, 生成本地证书, 将 CA 证书, 本地证书和 CRL 导入到内存中; 2.IPSEC 基本功能, 使 Enodeb 上线, SeGW 配置证书策略为符合 Enodeb dn 字段, 检查 IPSec 隧道是否建立成功; 3.IPSEC 基本功能, 配置证书策略为不符合 Enodeb dn 字段, 检查 IPSec 隧道是否建立成功
预期结果	1.证书和 CRL 导入到内存成功; 2.Enodeb 可以正常建立隧道, 业务转发正常; 3.Enodeb隧道建立失败

## 5.2.5 在线更新/增加证书业务不中断功能测试

测试项目	在线更新/增加证书业务不中断功能测试
测试内容	能够成功的进行在线更新/增加证书业务不中断功能
测试准备	1.SeGW 工作正常; 2.SeGw 开启 CRL 验证; 3.SeGW 与 CA、CRL 服务器可正常通信, 并且 CA、CRL 服务器支持 SCEP 协议
测试步骤	在线更新/增加证书过程中, 检查业务是否受到影响
预期结果	检查业务正常, 未受影响, SeGW 下载证书正常

## 5.2.6 使用 SCEP 下载证书/CRL

测试项目	测试 SCEP 下载证书/CRL 功能
测试内容	测试 SCEP 下载证书/CRL 功能
测试准备	1.SeGW 工作正常; 2.SeGw 开启 CRL 验证; 3.SeGW 与 CA、CRL 服务器可正常通信, 并且 CA、CRL 服务器支持 SCEP 协议
测试步骤	1.配置 PKI 实体信息; 2.配置 PKI 域信息参数 (含根证书指纹和 url 路径等); 3.使用 SCEP 下载 CA/RA 证书; 4.使用 SCEP 分别使用带外挑战字和无挑战字两种情况下载本地证书; 5.使用 SCEP 下载 CRL 测试
预期结果	CA/RA证书, 本地证书和 CRL均正常下载

## 5.2.7 使用 CMP 颁发证书

测试项目	使用 CMP 颁发证书
测试内容	测试 CMP IR, CR KUR 申请证书的功能
测试准备	SeGW 工作正常; SeGw 开启 CRL 验证; SeGW 与 CA、CRL 服务器可正常通信, 并且 CA 服务器支持 CMP 协议。
测试步骤	1.创建 CMP 会话信息 2.使用消息认证码的方式 IR 向 CMP 服务器申请本地证书 3.使用下载的 IR 证书作为认证证书, 进行 CR 证书申请 4.配置密钥重生成长度, 使用 KUR 方式更新证书
预期结果	三种方式下载证书功能正常

## 5.3 IPsec VPN 功能测试

## 5.3.1 IPsec 基本功能测试

测试项目	IPsec VPN 功能要求测试
测试内容	SeGW 支持 IPsec VPN
测试准备	1.SeGW、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.eNodeB 连上服务器, 中间穿过 SeGW; 2.eGW 上配置证书、保护的数据流等相关信息, 观察是否建立 IPsec 隧道
预期结果	eNodeB与SeGW之间能根据配置建立起相应的IPsec隧道

## 5.3.2 IKEv1 基本功能测试

测试项目	IKEv1 基本功能测试
测试内容	SeGW 支持 IKEv1 功能
测试准备	1.SeGW、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1. eNodeB 连接 SeGW 建立 IKEv1 的隧道; 2. 配置流量和时间重协商参数, 观察重协商功能是否正常; 3. 配置 DPD 参数, 观察隧道异常时, dpd 功能是否生效; 4. 配置 PFS 参数, 检查协商时是否受影响
预期结果	以上功能完全按照RFC标准实现, 满足功能需求



## 5.3.3 IKEv2 基本功能测试

测试项目	IKEv2 基本功能测试
测试内容	SeGW 支持 IKEv2 功能
测试准备	1.SeGW、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.eNodeB 连接 SeGW 建立 IKEV1 的隧道 2.配置流量和时间重协商参数, 观察重协商功能是否正常; 3.配置 DPD 参数, 观察隧道异常时, dpd 功能是否生效; 4.配置 PFS 参数, 检查协商时是否受影响; 5.配置 reauth 参数, 观察重认证功能是否正常
预期结果	以上功能完全按照RFC标准实现, 满足功能需求

## 5.3.4 IPSec 加密算法

测试项目	IPSec 加密算法
测试内容	验证 IPSec 能够选择正确的加密算法 (含非对称加密算法、对称加密算法和哈希算法)
测试准备	1.SeGW、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.配置 ipsec 相关配置, 遍历所支持的加密算法; 2.查看 enodeb 和 SeGW 在如上情况下, 是否能够正常协商
预期结果	隧道协商成功, 业务正常转发

## 5.3.5 多级证书 IPSec 协商

测试项目	多级证书 IPSec 协商
测试内容	验证支持多级证书的 IPsec 协商
测试准备	1.SeGW、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.SeGW 和 enodeb 通过 CA 服务器下载二级以上证书 (最多四级); 2.配置 ipsec 相关策略, 将证书绑定到 ipsec 策略中; 3.流量触发 enodeb 和 SeGW 建立隧道, 观察隧道是否正常建立
预期结果	隧道协商成功, 业务正常转发

## 5.3.6 反向路由注入功能测试

测试项目	反向路由注入功能测试
测试内容	测试 IPsec 隧道生成后，生成反向路由，引入动态路由协议
测试准备	1.SeGW、eNodeB 和服务器工作正常； 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.SeGW 使能 ipsec 反向路由注入功能； 2.Enodeb, SeGW 配置 ipsec 相关参数； 3.流量触发隧道建立； 4.查看是否生成反向路由，将反向路由分别引入 OSPF 和 BGP 中，查看对端设备是否可以通过动态路由协议学习到此路由
预期结果	隧道协商成功后，反向路由生成，通过动态路由发布正常

## 5.3.7 IKE 协商报文的 DSCP 修改

测试项目	IKE 协商报文修改 DSCP
测试内容	测试 IKE 协商报文可以根据配置进行修改
测试准备	1.SeGW、eNodeB 和服务器工作正常； 2.SeGW、eNodeB 和服务器之间可正常通信。
测试步骤	1.配置 SeGW 上的 IPsec 相关配置，并配置 IKE DSCP 值； 2.触发 enodeb 和 SeGW 建立隧道； 3.抓取 IKE 协商报文，查看协商报文 DSCP 值是否和配置一致
预期结果	IKE 协商报文的DSCP值跟配置一致

## 5.3.8 多 IPsec 策略协商隧道

测试项目	多 IPsec 策略协商隧道
测试内容	测试当配置多 IPsec 策略时，隧道协商功能；
测试准备	1.SeGW、eNodeB 和服务器工作正常； 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.SeGW 配置多个 ipsec proposal 应用于 policy 中； 2.enodeb 的 ipsec proposal 命中 SeGW 的最后一个选项； 3.触发 enodeb 和 SeGW 建立 ipsec 隧道
预期结果	IPsec隧道可以正常建立，业务转发正常

## 5.3.9 IPSec 隧道协商失败原因查看

测试项目	IPSec 隧道协商失败原因查看
测试内容	测试 IPSec 隧道协商失败原因查看
测试准备	1.SeGW、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.SeGW 和 enodeb 之间除 psk 配置不同外, 其他参数均正确; 2. enodeb 和 SeGW 触发协商; 3.使用查看命令查看隧道协商失败原因
预期结果	可以看到对应enodeb IP协商失败原因

## 5.3.10 IPSec 容灾测试

测试项目	IPSec 容灾测试
测试内容	测试网络异常的情况下, IPSec 对业务的影响
测试准备	1.SeGW 为双机设备、eNodeB 和服务器工作正常; 2.SeGW、eNodeB 和服务器之间可正常通信
测试步骤	1.两台 SeGW 组建双机环境, 配置相关 IPSec 配置; 2.enodeb 与 SeGW 公共隧道 IP 建立 ipsec 隧道; 3.业务正常转发下, down 掉防火墙上下行链路, 查看业务是否受影响
预期结果	可以看到流量切换到备SeGW设备上, 业务正常转发

## 5.4 攻击防范功能测试

## 5.4.1 攻击防范测试

## 5.4.1.1 ICMP ping of death 攻击防范测试

测试项目	ICMP ping of death 攻击防范测试
测试内容	ICMP ping of death 攻击防范测试
测试准备	1.SeGW、测试仪工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1. SeGW 上开启 ICMP ping of death 攻击防范功能; 2.测试仪器发送攻击流量
预期结果	ICMP ping of death 攻击流量被阻断并告警

## 5.4.1.2 Tear drop 攻击防范测试

测试项目	Tear drop 攻击防范测试
测试内容	Tear drop 攻击防范测试
测试准备	1.SeGW、测试仪工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 上开启 Tear drop 攻击防范功能； 2.测试仪器发送攻击流量
预期结果	Tear drop 攻击流量被阻断并告警

## 5.4.1.3 TCP syn flood 攻击防范测试

测试项目	TCP syn flood 攻击防范测试
测试内容	TCP syn flood 攻击防范测试
测试准备	1.SeGW、测试仪工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 上开启 TCP syn flood 攻击防范功能； 2.测试仪器发送攻击流量
预期结果	TCP syn flood 攻击流量被阻断并告警

## 5.4.1.4 TCP land 攻击防范测试

测试项目	TCP land 攻击防范测试
测试内容	TCP land 攻击防范测试
测试准备	1.SeGW、测试仪工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 上开启 TCP land 攻击防范功能； 2.测试仪器发送攻击流量
预期结果	TCP land 攻击流量被阻断并告警。



## 5.4.2 过滤功能测试

测试项目	ACL 过滤测试
测试内容	ACL 过滤测试
测试准备	1.SeGW、客户端和服务端工作正常； 2.SeGW、客户端和服务端之间可正常通信
测试步骤	1.SeGW 配置一条 ACL，ACL 中添加一条规则，该规则允许特定客户流量通过，比如端口号为 80 的流量； 2.SeGW 上使用上述 ACL 在域间配置包过滤策略； 3.客户端上发送多条流量到服务器
预期结果	只有命中 ACL 中规则的流量通过，其他流量被拒绝

## 5.5 路由支持功能测试

## 5.5.1 静态路由功能测试

测试项目	静态路由测试
测试内容	静态路由测试
测试准备	1.SeGW、客户端和服务端工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 上配置到客户端以及服务端端的静态路由； 2.客户端发送流量到服务器
预期结果	流量命中静态路由成功转发

## 5.5.2 OSPF 协议测试

测试项目	OSPF 协议测试
测试内容	OSPF 协议测试
测试准备	1.SeGW、路由器工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 和路由器之间起 OSPF 协议； 2.路由器上通过 OSPF 发布路由； 3.SeGW 上检查 OSPF 协议邻居状态和路由表项
预期结果	1.SeGW 上 OSPF 邻居状态为 FULL，SeGW 与路由器之间 OSPF 协议邻居协商成功； 2.SeGW 能学习到路由器通过 OSPF 发布的路由

## 5.5.3 OSPF 路由过滤测试

测试项目	OSPF 路由过滤
测试内容	SeGW 能对 OSPF 发布和学习到的路由过滤
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 与路由器之间配置 OSPF 路由协议; 2.路由器上 OSPF 路由进程下引入静态路由, 比如: 180.180.0.0/16; 3.SeGW 上配置基本 ACL 过滤 OSPF 学习到的路由到路由表, 比如 ACL 下配置规则拒绝静态路由 180.180.0.0/16。OSPF 进程下使用该 ACL 配置引入过滤策略; 4.SeGW 上 OSPF 进程下引入静态路由, 比如 190.190.0.0/16; 5.SeGW 上配置基本 ACL 过滤 OSPF 发布引入的路由到对端, 比如 ACL 下配置规则拒绝静态路由 190.190.0.0/16。OSPF 进程下使用该 ACL 配置发布过滤策略
预期结果	1.步骤 2, SeGW 上能通过 OSPF 学习到路由器发布的静态路由, 比如: 180.180.0.0/16; 2.步骤 3, SeGW 路由表内无路由器发布的静态路由, 比如: 180.180.0.0/16, SeGW 能过滤 OSPF 学习到的路由; 3.步骤 4, 路由器能学习到 SeGW 发布的静态路由, 比如: 190.190.0.0/16; 4.步骤 5, 路由器学习不到 SeGW 引入的静态路由, 比如: 190.190.0.0/16, SeGW 能过滤发布到对端的引入路由

## 5.5.4 OSPF stub 测试

测试项目	OSPF stub 测试
测试内容	OSPF stub 测试
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGWA、SeGWB 和路由器之间起 OSPF 协议; 2.路由器上引入静态路由到 OSPF 进程, 比如 200.200.0.0/16; 3.SeGWA 和 SeGWB 上配置 Area1 为 stub 区域; 4.SeGWB 上配置“stub no-summary”命令发布 LSA 3 类通告到 stub 区域
预期结果	1.步骤 2, SeGWA 上能学习到路由器发布的静态路由, 200.200.0.0/16。SeGWA 上 OSPF 链路状态数据库中存在 LSA 3 和 LSA 5 类通告; 2.步骤 3, 配置成 stub 区域后, SeGWA 上 OSPF 路由表中没有路由器发布的静态路由 200.200.0.0/16,取而代之的是一条默认路由。OSPF 链路状态数据库中没有 LSA 5 类通告; 3.步骤 4, SeGWA 上 OSPF 链路状态数据库中没有 LSA 3 类通告

## 5.5.5 OSPF 协议联动 BFD 测试

测试项目	OSPF 协议联动 BFD 测试
测试内容	OSPF 协议联动 BFD 测试。BFD 探测到链路故障时 OSPF 邻接关系立即变为 Down 而无需等待 OSPF DEAD TIMER 超时，促使路由快速收敛
测试准备	1.SeGW、路由器工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW和路由器之间起OSPF协议； 2.OSPF进程下开启BFD探测功能； 3.路由器上制造链路层或者转发层故障
预期结果	1.步骤 2,OSPF 邻接关系协商成功状态变为 FULL 后，会建立 BFD 联动的会话，状态为 Up； 2.步骤 3, BFD 探测到链路故障时 OSPF 邻接关系立即变为 DOWN 无需等待 OSPF DEAD TIMER 超时，促使路由快速收敛

## 5.5.6 IS-IS 协议测试

测试项目	IS-IS 协议测试
测试内容	IS-IS 协议测试
测试准备	1.SeGW、路由器工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 和路由器之间起 ISIS 协议； 2.路由器上通过 ISIS 发布路由； 3.SeGW 上检查 ISIS 协议邻居状态和路由表项
预期结果	1.SeGW 上 ISIS 邻居状态为 UP，SeGW 与路由器之间 ISIS 协议邻居协商成功； 2.SeGW 能学习到路由器通过 ISIS 协议发布的路由



## 5.5.7 IS-IS 路由过滤测试

测试项目	IS-IS 路由过滤
测试内容	IS-IS 路由过滤
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 与路由器之间配置 ISIS 路由协议; 2.路由器上 ISIS 路由进程下引入静态路由, 比如: 181.181.0.0/16 3.SeGW 上配置基本 ACL 过滤 ISIS 学习到的路由到路由表, 比如 ACL 下配置规则拒绝静态路由 181.181.0.0/16。OSPF 进程下使用该 ACL 配置引入过滤策略; 4.SeGW 上 ISIS 进程下引入静态路由, 比如 191.191.0.0/16; 5.SeGW 上配置基本 ACL 过滤 OSPF 发布引入的路由到对端, 比如 ACL 下配置规则拒绝静态路由 191.191.0.0/16。ISIS 进程下使用该 ACL 配置发布过滤策略
预期结果	1.步骤 2, SeGW 上能通过 ISIS 学习到路由器发布的静态路由, 比如: 181.181.0.0/16; 2.步骤 3, SeGW 路由表内无路由器发布的静态路由 181.181.0.0/16, SeGW 能过滤 ISIS 学习到的路由; 3.步骤 4, 路由器能学习到 SeGW 发布的静态路由, 比如: 191.191.0.0/16; 4.步骤 5, 路由器学习不到 SeGW 引入的静态路由, 比如: 191.191.0.0/16, SeGW 能过滤发布到对端的引入路由

## 5.5.8 IS-IS 协议联动 BFD 测试

测试项目	ISIS 协议联动 BFD 测试
测试内容	ISIS 协议联动 BFD 测试。BFD 探测到链路故障时 ISIS 邻接关系立即变为 Down 而无需等待 ISIS DEAD TIMER 超时, 促使路由快速收敛
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW和路由器之间起ISIS协议; 2.ISIS进程下开启BFD探测功能; 3.路由器上制造链路层或者转发层故障
预期结果	1.步骤 2,ISIS 邻接关系协商成功状态变为 UP 后, 会建立 BFD 联动的会话, 状态为 Up; 2.步骤 3, BFD 探测到链路故障时 ISIS 邻接关系立即变为 DOWN 无需等待 ISIS DEAD TIMER 超时, 促使路由快速收敛



## 5.5.9 BGP 协议测试

测试项目	BGP 协议测试
测试内容	BGP 协议测试
测试准备	1.SeGW、路由器工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 和路由器 A 之间起 EBGP 协议，SeGW 和路由器 B 之间起 IBGP 协议； 2.路由器上通过 BGP 发布路由； 3. SeGW 上查看 BGP 状态和 BGP 路由表
预期结果	1.SeGW 上 EBGP 和 IBGP 状态为 Established，SeGW 和路由器成功建立 EBGP 和 IBGP 邻居关系； 2.SeGW 能通过 BGP 学习到对端的路由

## 5.5.10 BGP 路由过滤测试

测试项目	BGP 路由过滤
测试内容	BGP 路由过滤
测试准备	1.SeGW、路由器工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 和路由器 A 之间起 EBGP 协议，SeGW 和路由器 B 之间起 IBGP 协议； 2.路由器上 BGP 进程下引入静态路由到 BGP 路由表，比如：182.182.0.0/16； 3.SeGW 上配置基本 ACL 过滤 BGP 学习到的路由到路由表，比如 ACL 下配置规则拒绝静态路由 182.182.0.0/16。BGP 进程下使用该 ACL 配置引入过滤策略； 4.SeGW 上 BGP 进程下引入静态路由，比如 192.192.0.0/16； 5.SeGW 上配置基本 ACL 过滤 BGP 发布的路由到对端，比如 ACL 下配置规则拒绝静态路由 192.192.0.0/16。BGP 进程下使用该 ACL 配置发布过滤策略
预期结果	1.步骤 2，SeGW 上能通过 BGP 学习到路由器发布的静态路由，比如：182.182.0.0/16； 2.步骤 3，SeGW 路由表内无路由器发布的静态路由，比如：182.182.0.0/16，SeGW 能过滤 OSPF 学习到的路由； 3.步骤 4，路由器能学习到 SeGW 发布的静态路由，比如：192.192.0.0/16； 4.步骤 5，路由器学习不到 SeGW 引入的静态路由，比如：192.192.0.0/16，SeGW 能过滤发布到对端的引入路由

## 5.5.11 BGP 协议联动 BFD 测试

测试项目	BGP 协议联动 BFD
测试内容	BGP 协议联动 BFD (Bidirectional Forwarding Detection).当 BFD 会话 down 掉时, BGP 邻接关系立即变为 down
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 和路由器之间起 BGP 协议; 2.BGP 进程下开启 BFD 探测功能; 3.路由器上制造链路层或者转发层故障
预期结果	1.步骤 2,BGP 邻居关系协商成功状态变为 Established 后, 会建立 BFD 联动的会话, 状态为 Up; 2.步骤 3, BFD 探测到链路故障时 BGP 邻接关系立即变为 DOWN 无需等待 BGP DEAD TIMER 超时, 促使路由快速收敛

## 5.5.12 策略路由测试

测试项目	策略路由测试
测试内容	策略路由测试
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW上配置两个出接口, 默认出接口为接口A, 另一个出接口为接口B; 2.客户端发送流量到服务器端, 中间穿越SeGW; 3.SeGW上配置ACL分流走策略路由的流量, 使用该ACL创建策略路由, 策略路由出接口为接口B; 4.流量入接口上应用上述配置的策略路由; 5.客户端发送流量到服务器端, 中间穿越SeGW
预期结果	1.步骤 2, 流量转发正常, 从 SeGW 接口 A 出去; 2.步骤 5, 命中策略路由 ACL 的流量从接口 B 出去, 其他流量从默认接口 A 出去

## 5.5.13 最大路由条目数测试

测试项目	最大路由条目数测试
测试内容	最大路由条目数测试
测试准备	1.SeGW、测试仪器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 和测试仪器之间起 BGP 协议; 2.配置测试仪器发布最大路由条目数到 SeGW, SeGW 路由表项最多可支持 200000 条; 3.查看 SeGW 上路由表项
预期结果	SeGW 路由表项达到最大时工作正常

## 5.5.14 多路由协议间路由引入测试

测试项目	多路由协议间路由引入
测试内容	多路由协议间路由引入
测试准备	1.SeGW、路由器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGWA 和 SeGWB 之间起 BGP 协议, SeGWB 和 SeGWC 之间起 OSPF 协议; 2.SeGWB 上 OSPF 进程下引入静态路由, 比如: 194.194.0.0、16, 同时引入 BGP 路由到 OSPF 进程; 3.SeGWC 上 BGP 进程下引入静态路由, 比如: 195.195.0.0、16; 4.4. 查看 SeGW 上的路由表
预期结果	1.SeGWB 上能通过 BGP 学习到 SeGWC 上 BGP 进程引入的静态路由, 比如: 195.195.0.0、16; 2.SeGWA 上能通过 OSPF 学习到 SeGWB 上 OSPF 进程引入的静态路由, 比如 194.194.0.0、16; 同时能学习到 SeGWB OSPF 引入的 BGP 路由

## 5.6 IPv6 功能测试

## 5.6.1 IPv6/IPv4 双栈测试

测试项目	IPv4/IPv6 双栈测试
测试内容	支持 IPv4/IPv6 双栈, IPv4 和 IPv6 协议能各自独立运行
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上开启 IPv6 功能; 2.接口下同时配置 IPv4 和 IPv6 地址; 3.SeGW 上同时配置到达客户端和服务端端的 IPv6 和 IPv4 的路由; 4.客户端发送同时发送 IPv4 和 IPv6 的流量到服务器, 中间穿过 SeGW
预期结果	IPv4和IPv6流量转发成功, IPv4和IPv6互不影响

## 5.6.2 IPv6 包过滤测试

测试项目	IPv6 包过滤
测试内容	SeGW 使用 ACL 实现 IPv6 包过滤。扩展 ACL 的规则可以配置源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议等; 基本 ACL 的规则可以配置源 IP 字段
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW配置一个扩展ACL, ACL下面配置一个允许通过规则, 规则包括源IP地址、源端口号、目的IP地址、目的端口号、协议字段; 2.SeGW上域间使用上面的ACL配置IPv6包过滤策略; 3.客户端上发送流量到服务器, 中间穿过SeGW; 4.SeGW上配置一个基本ACL, ACL下面配置一个允许通过规则, 规则包括源IP地址; 5.SeGW上域间使用上面的ACL配置IPv6包过滤策略; 6.客户端上发送流量到服务器, 中间穿过SeGW
预期结果	1.步骤 3, 只有匹配 ACL 的 IPv6 流量通过, 其他流量被拒绝; 2.只有匹配 ACL 的 IPv6 流量通过, 其他流量被拒绝



## 5.7 地址转换功能测试

## 5.7.1 NAT-NOPAT 测试

测试项目	NAT-NOPAT 测试
测试内容	NAT-NOPAT 测试
测试准备	SeGW、客户端和服务端工作正常; 接口下配置 IP 地址并加入安全域; 包过滤为允许通过。
测试步骤	1.SeGW 配置一条 ACL 分流需要做 NAT-NOPAT 的流量; 2.SeGW 配置一个 NAT 地址池, 地址池里面包含多个公有地址; 3.SeGW 上域间使用上述 ACL 和地址池配置 NAT-NOPAT 策略; 4.客户端上发送匹配 ACL 的流量到服务器, 中间穿过 SeGW。
预期结果	1. 流量通且无丢失。SeGW 上将私有地址做一对一转换成公有地址, 只转 IP 地址不转端口号。SeGW 上建立 NAT 会话表项记录地址转换信息。

## 5.7.2 目的 NAT 测试

测试项目	目的 NAT
测试内容	SeGW 能转换目的地址
测试准备	1.SeGW、客户端和服务端工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置 NAT Server, 将目的地址转换成指定的地址; 2.客户端发送目的地址匹配 NAT server 表项的流量到服务器, 中间穿过 SeGW
预期结果	流量通且无丢失。SeGW 上目的地址转换成指定的目的地址, 建立会话表项记录地址转换信息

## 5.7.3 NAT PAT 多对一转换测试

测试项目	NAT PAT 多对一转换
测试内容	SeGW 能做 NAT PAT 转换, 并且多个私有地址共用一个公有地址
测试准备	1.SeGW、客户端和服务端工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1. SeGW 上配置一条 ACL 分流做 NAT PAT 的流量; 2. SeGW 上配置一个 NAT 地址池, 该地址池只包含一个公有地址; 3. SeGW 上域间使用上述 ACL 和地址池配置 NAT PAT 策略; 4.客户端上发送多条变化源地址的流量到服务器, 中间穿过 SeGW
预期结果	流量通且无丢失。SeGW 将私有地址转换成公有地址, 并且多个私有地址通过端口转换共享一个公有地址。SeGW 建立会话表项记录地址转换信息

## 5.7.4 NAT PAT 多对多转换测试

测试项目	NAT PAT 多对多转换
测试内容	NAT PAT 多对多转换
测试准备	1.SeGW、客户端和服务端工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置一条 ACL 分流做 NAT PAT 的流量; 2.SeGW 上配置一个 NAT 地址池, 该地址池只包含多个公有地址; 3.SeGW 上域间使用上述 ACL 和地址池配置 NAT PAT 策略; 4.客户端上发送多条变化源地址的流量到服务器, 中间穿过 SeGW
预期结果	流量通且无丢失。SeGW 将私有地址转换成公有地址, 并且转换端口地址实现 IP 公有地址共享。SeGW 建立会话表项记录地址转换信息

## 5.7.5 Smart NOPAT 测试

测试项目	Smart NO-PAT
测试内容	地址池包含多个公有地址, 优先做 NAT NOPAT 转换, 地址不够用时最后一个地址做 PAT 转换
测试准备	1.SeGW、客户端和服务端工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置一条 ACL 分流做 NAT 的流量; 2.SeGW 上配置一个 NAT 地址池, 该地址池只包含多个公有地址, 并开启 Smart NOPAT 功能; 3.SeGW 上域间使用上述 ACL 和地址池配置 NAT NO-PAT 策略; 4.客户端上发送多条变化源地址的流量到服务器, 中间穿过 SeGW
预期结果	流量通且无丢失。SeGW 优先做 NO PAT 转换将私有地址一对一转换成公有地址, 当地址不够用使用地址池里面最后一个地址做 PAT 转换, 多个私有地址共享一个公有地址。SeGW 建立会话表项记录地址转换信息

## 5.7.6 NAT 转换控制特性测试

测试项目	NAT 转换控制特性测试
测试内容	NAT 转换控制特性测试
测试准备	1.SeGW、客户端和服务端工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置一条 ACL 分流做 NAT 的流量; 2.SeGW 上配置一个 NAT 地址池, 地址池包含多个公有地址; 3.SeGW 上域间使用上述 ACL 和地址池配置 NAT PAT 策略; 4.客户端上发送源地址不变源端口变化的多条流量到服务器, 中间穿过 SeGW
预期结果	具有相同源地址的不同流总是被转换成相同的公有地址

## 5.7.7 NAT 地址转换表项生存时间可配置测试

测试项目	NAT 地址转换表项生存时间可配置测试
测试内容	NAT 地址转换表项生存时间是可配置的
测试准备	1.SeGW、客户端和服务端工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上域间使用 ACL 和地址池配置 NAT 策略; 2.客户端上发送流量到服务器, 中间穿过 SeGW; 3.停止流量, 清空会话表项, 修改 NAT 地址转换表项生存时间; 4.客户端上重新发送流量到服务器, 中间穿过 SeGW
预期结果	1.步骤2, 流量在 SeGW 做 NAT 转换, SeGW 建立会话表项记录地址转换信息, 会话表项里包含表项默认生存时间; 2.步骤4, 会话表项生存时间更改为配置的时间



## 5.8 可靠性功能测试

## 5.8.1 双控制平面冗余测试

测试项目	双控制平面冗余测试
测试内容	双控制平面冗余测试
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过; 4.如果使用动态路由协议需要开启动态路由协议 GR 功能
测试步骤	1.客户端发送流量到服务器,中间穿过 SeGW; 2.重启或者拔出主主控版; 3.检查流量
预期结果	主主控故障时备主控切换为新的主主控,切换过程中流量不受影响

## 5.8.2 电源冗余测试

测试项目	电源冗余测试
测试内容	电源冗余测试
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.客户端发送流量到服务器,中间穿过 SeGW; 2.拔掉其中一个电源 3.重新插入电源
预期结果	电源插拔过程中流量不受任何影响

## 5.8.3 双机热备份时整机故障切换测试

测试项目	双机热备份时整机故障切换测试
测试内容	双机热备份时整机故障切换测试
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.两台 SeGW 之间启动双机热备份功能并配置心跳线; 2.客户端上从服务器上 FTP 下载一个大文件,中间穿过主设备; 3.主设备下电,查看设备状态和 FTP 业务
预期结果	整机故障时 SeGW 发生主备切换,FTP 业务不受影响,正在下载的任务能成功完成



## 5.8.4 双机热备份时链路故障切换测试

测试项目	双机热备份时链路故障切换测试
测试内容	双机热备份时链路故障切换测试
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.两台 SeGW 之间启动双机热备份功能并配置心跳线; 2.客户端上从服务器上 FTP 下载一个大文件,中间穿过主设备; 3.主设备上制造链路故障,查看设备状态和 FTP 业务
预期结果	整机故障时 SeGW 发生主备切换,FTP 业务不受影响,正在下载的任务能成功完成

## 5.8.5 双机热备份时主设备自动备份配置到备设备测试

测试项目	双机热备份时主设备自动备份配置到备设备测试
测试内容	双机热备份时主设备自动备份配置到备设备测试
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.两台 SeGW 之间开启双机热备份功能并配置心跳线; 2.主 SeGW 上配置 ACL、地址池地址等配置; 3.主 SeGW 上保存配置
预期结果	1.步骤 2,主设备自动备份配置到备设备; 2.步骤 3,备设备自动保存配置

## 5.8.6 VRRP 测试

测试项目	VRRP 测试
测试内容	两台 SeGW 上的接口起 VRRP 协议,主接口故障时备接口切换为新的主接口
测试准备	1.SeGW 工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.两台 SeGW 开启 HRP 功能,并配置心跳线; 2.两台 SeGW 上的接口起 VRRP 协议,将客户端上的默认网关配置为 VRRP 的虚拟 IP 地址; 3.客户端上发送流量到服务器,中间经过主接口穿过 SeGW; 4.拔掉主接口,查看流量
预期结果	主接口故障后备接口切换为主接口,流量从备接口穿过,流量几乎不受影响

## 5.9 配置管理功能测试

测试项目	管理配置文件测试
测试内容	在进行管理配置文件的配置，了解此特性的应用环境、配置此特性的前置任务和数据准备，测试是否可以快速、准确地完成配置任务
测试准备	安装完毕并上电启动正常
测试步骤	1.为了让正常启动，用户需要正确选择在启动时加载的系统软件和配置文件。 2.用户在修改当前配置后，需要保存修改的内容。 3.用户需要查看的配置信息
预期结果	完成配置任务

## 5.10 日志告警测试

## 5.10.1 TCP 会话日志测试

测试项目	TCP 会话日志测试
测试内容	TCP 会话日志测试
测试准备	1.SeGW、客户端、服务器、Log 服务器工作正常； 2.接口下配置 IP 地址并加入安全域； 3.包过滤为允许通过
测试步骤	1.SeGW 上配置日志服务器； 2.SeGW 配置一个 ACL 用于过滤需要发送会话日志的流量； 3.SeGW 域间使用上述 ACL 配置会话日志策略； 4.客户端上发送 TCP 流量到服务器端，中间穿过 SeGW； 5.清除会话或者等待会话老化； 6.Log 日志上查看日志
预期结果	Log 日志服务器上存在 TCP 会话的日志，日志中包含流量的源 IP、源端口号、目的 IP、目的端口号、协议等信息。如果流量做了 NAT 地址转换日志信息中也包含地址转换信息

## 5.10.2 UDP 会话日志测试

测试项目	UDP 会话日志测试
测试内容	UDP 会话日志测试
测试准备	1.SeGW、客户端、服务器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置日志服务器; 2.SeGW 配置一个 ACL 用于过滤需要发送会话日志的流量; 3.SeGW 域间使用上述 ACL 配置会话日志策略; 4.客户端上发送 UDP 流量到服务器端,中间穿过 SeGW; 5.清除会话或者等待会话老化; 6.Log 日志上查看日志
预期结果	Log 日志服务器上存在 UDP 会话的日志,日志中包含流量的源 IP、源端口号、目的 IP、目的端口号、协议等信息。如果流量做了 NAT 地址转换日志信息中也包含地址转换信息

## 5.10.3 ICMP 会话日志测试

测试项目	ICMP 会话日志测试
测试内容	ICMP 会话日志测试
测试准备	SeGW、客户端、服务器工作正常; 接口下配置 IP 地址并加入安全域; 包过滤为允许通过
测试步骤	1.SeGW 上配置日志服务器; 2.SeGW 配置一个 ACL 用于过滤需要发送会话日志的流量; 3.SeGW 域间使用上述 ACL 配置会话日志策略; 4.客户端上发送 ICMP 流量到服务器端,中间穿过 SeGW; 5.清除会话或者等待会话老化; 6.Log 日志上查看日志
预期结果	Log 日志服务器上存在 ICMP 会话的日志,日志中包含流量的源 IP、源端口号、目的 IP、目的端口号、协议等信息。如果流量做了 NAT 地址转换日志信息中也包含地址转换信息

## 5.10.4 系统日志测试

测试项目	系统日志
测试内容	系统日志
测试准备	1.SeGW、客户端、服务器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置系统日志服务器; 2.制造不同级别的系统日志; 3.系统日志服务器上查看日志
预期结果	日志服务器上存在相关系统日志, 且分级别

## 5.10.5 SNMP walk 测试

测试项目	SNMP walk 测试
测试内容	SNMP walk 测试
测试准备	1.SeGW、客户端、SNMP 网管服务器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置 SNMP 网管服务器; 2.服务器上执行 Walk 命令查看节点
预期结果	能查看所有 MIB 节点

## 5.10.6 链路故障时向网管发送告警测试

测试项目	链路故障时向网管发送告警测试
测试内容	链路故障时向网管发送告警测试
测试准备	1.SeGW、客户端、SNMP 网管服务器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置 SNMP 网管服务器; 2.SeGW 制造链路故障
预期结果	SNMP 网管服务器上收到链路故障告警



## 5.10.7 设备整机下电时向网管发送告警测试

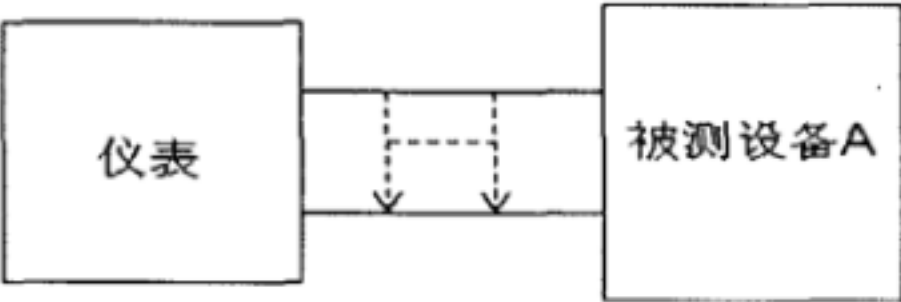
测试项目	设备整机下电时向网管发送告警测试
测试内容	设备整机下电时向网管发送告警测试
测试准备	1.SeGW、客户端、SNMP 网管服务器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.SeGW 上配置 SNMP 网管服务器; 2.给设备下电
预期结果	SNMP 网管服务器上收到设备故障告警

## 5.10.8 双机热备份切换时向网管发送告警测试

测试项目	双机热备份切换时向网管发送告警测试
测试内容	双机热备份切换时向网管发送告警测试
测试准备	1.SeGW、客户端、SNMP 网管服务器工作正常; 2.接口下配置 IP 地址并加入安全域; 3.包过滤为允许通过
测试步骤	1.两台 SeGW 之间开启双机热备份功能并配置心跳线; 2.SeGW 上配置 SNMP 网管服务器; 3.制造故障时双机热备份发生主备切换,网管服务器上查看告警
预期结果	双机热备份切换时网管能收到告警

6 性能测试

6.1 IPSec 并发连接数与新建连接数测试

测试项目	IPSec 并发连接数和新建连接数测试
测试内容	IPSec 并发连接数和新建连接数测试
测试准备	<p>1.设备和仪表连接如下，中间连线数量与设备性能和仪表性能相关，请根据实际情况进行连接；</p> <div data-bbox="953 706 1549 905"></div> <p>2.SeGW、仪表接口下配置 IP 地址并加入安全域；</p> <p>3.SeGW 包过滤为允许通过</p>
测试步骤	<p>1.使用仪表（例如：Avalanche 等）和 SeGW 建立 IPSec VPN 隧道（Remote）</p> <p>2.IKE 相关协商参数（加密算法，认证算法，完整性算法，DH 组）根据实际要求配置；</p> <p>3.使用仪表测试 SeGW IPSec VPN 最大并发连接数</p> <p>4.使用仪表测试 SeGW IPSec VPN （预共享密钥方式）最大新建连接数，查看新建速率稳定后的最大新建连接数；</p> <p>5.使用仪表测试 SeGW IPSec VPN （1024 密钥长度或 2048 密钥长度 证书方式）最大新建连接数，查看新建速率稳定后的最大新建连接数</p>
预期结果	记录最大并发连接数，每秒最大新建连接数

## 6.2 IPsec 吞吐量和时延测试

测试项目	IPsec 吞吐量和时延测试
测试内容	IPsec 吞吐量和时延测试
测试准备	<p>1.设备和仪表连接如下，中间连线数量与设备性能和仪表性能相关，请根据实际情况进行连接；</p> <div data-bbox="947 685 1543 1083" data-label="Diagram"> <pre> graph TD     Instrument[仪表] --&gt; DeviceA[被测设备A]     Instrument --&gt; DeviceB[被测设备B]     DeviceA --- DeviceB     </pre> </div> <p>2.SeGW、仪表接口下配置 IP 地址并加入安全域；</p> <p>3.SeGW 包过滤为允许通过</p>
测试步骤	<p>1.使用仪表（例如：IXIA，TestCenter 等）发送二三层流量，触发被测设备 A 和被测设备 B 之间 IPsec 隧道；</p> <p>2.IPsec 相关协商参数（加密算法，认证算法）根据实际要求配置，例如 AES128，AES256，SHA1 等；</p> <p>3.使用仪表分别发送不同字节大小的报文，测试 SeGW 不同字节的处理能力，例如 64,128,256,512,1024,1280,1420,1518 字节和 IMIX 测试；</p> <p>4.被测设备之间建立隧道时，采用多条隧道进行加密流量的方式测试，建议采用 4 的倍数或 2 的指数幂的隧道数量进行测试</p>
预期结果	记录被测设备的最大吞吐量大小和对应的时延信息，以及规定时延范围内的吞吐量大小

## 参 考 文 献

- [1]3GPP TS 33.401, Security architecture
  - [2]3GPP TS 33.210, IP network layer security
  - [3]3GPP TS 33.310, Authentication Framework (AF)
  - [4]IETF RFC4301, Security Architecture for The Internet Protocol
  - [5]IETF RFC4306, Internet Key Exchange (IKEv2) Protocol
  - [6]IETF RFC4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
  - [7]RFC2338虚拟路由冗余协议 (Virtual Router Redundancy Protocol) (version number One 1998)
  - [8]RFC3768虚拟路由冗余协议 (Virtual Router Redundancy Protocol) (version number Two 2004)
  - [9]RFC1631IP网络地址转换
  - [10]RFC2663IP NAT术语及考虑
  - [11] GB/T 20010-2005, 信息安全技术 包过滤防火墙评估准则
  - [12] GB/T 18019-1999, 信息技术 应用级防火墙安全技术要求
  - [13] GB/T 18020-1999, 信息技术 包过滤防火墙安全技术要求
  - [14]YD/T 1132-2001, 防火墙设备技术要求
-



中华人民共和国  
通信行业标准  
LTE 无线网络安全网关测试方法  
YD/T 2874-2015

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路11号邮电出版大厦  
邮政编码：100164  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16 2016年3月第1版  
印张：2.25 2016年3月北京第1次印刷  
字数：61千字

15115·785

定价：25元

本书如有印装质量问题，请与本社联系 电话：(010)81055492