ICS 33.040
M 15

YD

中华人民共和国通信行业标准

YD/T 2853-2015

LTE 无线网络安全网关技术要求

Technical requirements for security gateway in LTE network

2015-04-30 发布　　2015-07-01 实施

中华人民共和国工业和信息化部　发布

目　　次

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）YD/T 2853《LTE无线网络安全网关技术要求》；

b）《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无线网络安全网关技术要求

1 范围

本标准规定了LTE无线网络环境安全网关设备或系统的功能要求和性能指标。

本标准适用于LTE无线网络环境安全网关设备或系统的设计、开发、测试和评价。

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

服务网关 Servinggateway

与用户平面有关，从功能上来说，是连接E-UTRAN的分组数据接口的终点。

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。

ACL	Access Control List	访问控制列表
AH	Authentication Head	认证报头协议
APN	Access Point Name	接入点
BFD	Bidirectional Forwarding Detection	双向转发检测
BGP	Border Gateway Protocol	边界网关协议
CA	Certificate Authority	数字证书认证中心
CMPv2	Certificate Management Protocol Version 2	证书管理协议版本二
CRL	Certificate Revocation List	证书吊销列表
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DPD	Digital Pre-Distortion	数字预失真
EPC	Evolved Packet Core	演进核心网
DSCP	Differentiated Services Code Point	差分服务代码点
ESP	Encapsulating Security Payload	封装安全载荷
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	演进的无线接入网
FTP	File Transfer Protocol	文件传输协议
GTP	GPRS Tunneling Protocol	GPRS 隧道协议

HTTP	Hypertext Transfer Protocol	超文本传送协议
HTTPS	HTTP over Secure Socket Layer	HTTP 安全版
IKE	Internet Key Exchange	因特网密钥交换协议
IMSI	International Mobile Subscriber Identification Number	国际移动用户识别码
IPSEC	IP Security Protocol	因特网安全协议
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统
LDAP	Lightweight Directory Access Protocol	轻量目录访问协议
MME	Mobility Management Entity	移动性管理实体
NAT	Network Address Translation	网络地址转换
OSPF	Open Shortest Path First	开放最短路径优先
PFS	Perfect Forward Security	完美前向安全
PKI	Public Key Infrastructure	公钥基础设施
PSK	Phase-Shift Keying	相移键控
RA	Register Authority	证书注册审批系统
RSA	Ron Rivest,Adi Shamir,Leonard Adleman 提出	公钥加密算法
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	Security Gateway	安全网关
SFTP	Secure File Transfer Protocol	安全文件传送协议
S-GW	Serving Gateway	服务网关
SSH	Secure Shell	安全外壳协议
SYSLOG	System Logical	系统逻辑
UE	User Equipment	用户设备
VGMP	VRRP Group Management Protocol	VRRP 组管理协议
VPN	Virtual Private Network	虚拟专用网
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

4 技术要求

4.1 功能要求

在EPC网络和eNodeB基站之间部署安全网关（SeGW），该安全网关一方面作为IPSec GW，对eNodeB和核心网之间的数据进行加密保护，对LTE接口之间的数据进行加密传输；另一方面在核心网边界部署安全网关，除了提供IPSec GW的功能外，还可以起到防火墙的作用，进行域间隔离，防止DDoS攻击。安全网关可以针对LTE的业务承载协议进行检测，比如GTP协议；可以对GTP恶意报文进行过滤，保护EPC网络设备的CPU资源和带宽。

4.1.1 IPSec VPN 功能要求

SeGW 应具备 IPSec VPN 功能，具体技术要求如下：

a）支持以 IPSec 协议（支持 AH、ESP、隧道模式、传输模式）为基础构建 VPN；

b）支持 IKEv1，支持时间和流量重协商、DPD、PFS；

c）支持 IKEv2,，支持时间和流量 rekey、reauth、DPD、PFS；

d）支持建立 VPN 的“远程接入”方式（模式配置，地址分配），可选支持“网关至网关”方式；

e）支持预共享密钥和 X.509 数字证书两种身份认证方式，EAP 认证；在远端接入场景下，支持针对不同终端的采用不同的 PSK 密钥或证书认证方式（多点接入）；

f）支持基于安全策略的安全保护；

g）安全网关所使用的密码算法（包括对称密码算法、非对称密码算法、哈希算法）应符合国家商用密码算法标准；

h）支持硬件随机数发生器生成密钥材料；

i）支持 IPv6 over IPv4 及 IPv4 over IPv6 的 IPSec 的隧道封装；

j）支持 IPv6 的 IPSec；

k）支持 IPSec VPN 的双机热备，支持 IPsec 的状态同步，支持主备和负载分担；

l）支持与 OSPF，BGP 动态路由结合的反向路由注入功能；

m）支持多级证书（4 级），支持交叉认证，支持多个 CA 系统；

n）支持 IPSec 多实例；

o）日志及网管告警：证书下载，更新，删除，到期提醒；

p）支持多密钥对，RSA 密钥对自动更新；

q）支持基站之间接口 X2 业务模型；

r）支持 IPSec 防重放窗口，大小可配，功能可关闭；

s）支持先分片后加密和先加密后分片，可配；

t）支持逻辑接口应用 IPSec 策略；

u）支持 IPSec 多策略（多个 proposal）；

v）支持 IKEv2 Redirect；

w）IPSecNAT 穿越；

x）支持 IKE 协商报文的 DSCP 优先级调整；

y）支持 IPSec 隧道协商失败原因查看。

4.1.2 PKI 功能要求

为了保证良好地支持IPsec VPN功能，安全网关应支持PKI机制。

4.1.2.1 证书申请、撤销、更新

在 SeGW 与对端设备建立安全连接之前，必须首先获取设备本身证书，对端设备使用该证书对 SeGW 进行身份认证。

当 SeGW 管理员发现设备被废除或者私钥泄漏并且证书未到期时，需要向 CA/RA 申请吊销本设备证书，并及时更新发布 CRL，防止设备证书和私钥被非法使用。

证书是有期限的，在证书到期后需要更新证书。SeGW 设备证书到期后将不能完成身份认证功能，必须更新。

4.1.2.2 CRL 分发

在PKI架构中，CRL中的证书是已经被吊销的证书，位于该列表中的证书是不可信的。用证书认证对端身份时，需要检查对端的证书是否在CRL中，因此SeGW应支持获取CRL。

4.1.2.3 证书管理

支持SCEP、CMPv2证书管理协议，支持LDAP、FTP、SFTP、HTTP等方式下载证书和CRL。

支持证书的属性过滤。

支持使用OCSP、CRL、none等多种方式及其组合检查证书是否失效。

4.1.2.4 交叉证书管理

若需要认证的设备证书不是同一个CA颁发的，此时想要验证对端设备的身份，可以使用交叉证书。交叉证书和普通设备证书一样，也需要对其进行生命周期管理，包括证书的申请、更新，撤销等。SeGW需要满足该要求，运营商是否使用，由运营商根据其实际情况而定。

4.1.2.5 在线更新/增加证书时业务不中断

SeGW 设备在与对端设备建立安全连接的时候可能发生申请证书、更新证书、撤销证书、获取 CRL，更新 CRL 等操作，这些操作不应该影响已经建立的 IPSec 业务。

4.1.2.6 在线更新/增加证书异常处理

SeGW 设备在进行证书申请、证书更新、证书撤销、获取 CRL、更新 CRL 等管理操作时可能发生错误而导致失败，SeGW 设备应具有能对这种异常进行处理的能力。

4.1.3 攻击防范

4.1.3.1 检测功能

SeGW应具有对SCTP报文进行状态检测及包过滤的功能，应具有对SCTP异常报文进行识别过滤的功能，防止恶意和非法的报文到达EPC核心网，消耗EPC网元资源，影响正常业务的使用。

4.1.3.2 攻击防范

SeGW应支持检测以下攻击行为：Ping-of-Death、Fraggle、圣诞树攻击、Winnuke；Flood类攻击防御：syn-flood、icmp-flood、http-flood、NTP Flood；

4.1.4 GTP 防护

4.1.4.1 内容过滤

SeGW应具有根据GTP报文内容进行过滤的功能，例如根据GTP报文中的APN、IMSI前缀等进行过滤，以使得指定用户才可使用网络资源。

4.1.4.2 消息类型过滤

SeGW应具有根据GTP消息类型进行过滤的功能，应具有可根据指定GTP版本、指定GTP消息类型进行过滤的功能，防止非期望的报文到达EPC核心网，消耗网络资源。

4.1.5 路由支持

4.1.5.1 静态路由

SeGW应支持静态路由协议。

4.1.5.2 OSPF

SeGW应支持OSPF协议。

SeGW应支持OSPFv3协议。

4.1.5.3 IS-IS

SeGW应支持IS-IS动态路由协议。

SeGW应支持IS-ISv6动态路由协议。

4.1.5.4 BGP

SeGW应支持BGP协议。

SeGW应支持BGP4+协议。

4.1.5.5 策略路由

SeGW应支持策略路由，能够根据源接口、源地址、目的地址、协议、端口以及时间范围配置策略路由，控制数据包的转发路径。

4.1.6 IPv6

4.1.6.1 双协议栈

SeGW应支持IPv4/IPv6双协议栈。

4.1.6.2 IPv6 包过滤

SeGW应具有IPv6 包过滤功能。应能根据源路由方式对IP包进行过滤，建议包过滤默认设置为丢弃所有源路由选择方式的数据包。

4.1.7 地址转换功能

4.1.7.1 NAT-NOPAT

SeGW应支持NAT-NOPAT，即一对一地址转换。在地址转换过程中，数据包的源IP地址由私网地址转换为公网地址，这种地址转换关系是一一对应的。

4.1.7.2 目的 NAT

SeGW应支持目的网络地址转换（NAT）功能。

4.1.7.3 源 NAT

SeGW应支持网络端口地址转换功能，可以解决多个私网IP地址同时映射为少数或一个公网IP地址的问题。

4.1.7.4 Smart NAT

SeGW应支持灵活的NAT配置方式——Smart NAT。主要实现的功能是：Smart No-PAT、NAT地址池中排除IP地址或端口、转换NAT地址池或地址池组状态。

4.1.8 可靠性要求

4.1.8.1 双机热备

SeGW应支持主—主模式双机热备或主—备模式双机热备两种方式。其中主—主模式双机热备是两台设备同时工作。其中一台设备出现故障的时候，另一台设备能接管故障设备的工作；主—备模式双机热备是同时只有一台设备进行工作。当主设备出现故障的时候，备用设备应能切换为主设备继续工作。无论哪种方式，SeGW都应支持配置同步以及状态同步。

4.1.8.2 VRRP

SeGW应支持VRRP虚拟路由冗余协议。

4.1.8.3 VGMP

SeGW应支持VGMP协议。

4.1.8.4 链路检测

SeGW应支持IP-link检测和BFD检测功能，检测链路状态。

4.1.9 配置管理

4.1.9.1 图形管理界面

应支持通过图形管理界面对SeGW进行配置管理，图形管理界面能够提供在线帮助文档。

4.1.9.2 CLI 管理界面

应支持通过CLI管理界面对SeGW进行配置管理。

4.1.9.3 远程管理安全

SeGW应支持加密的远程管理，包括SSH、HTTPS等。

4.1.9.4 管理员身份鉴别

SeGW应支持管理员身份鉴别，只有通过身份鉴别的管理员才能对SeGW进行配置管理。

4.1.9.5 配置管理日志

SeGW应支持对配置过程产生日志。

4.1.9.6 管理员权限划分

SeGW应支持对管理员的权限进行划分，不同的管理员具有不同的权限。支持监视、配置、管理权限。

4.1.10 日志管理

4.1.10.1 日志发送

SeGW应支持按照SYSLOG标准发送日志到指定服务器。

4.1.10.2 日志存储

SeGW应支持保存日志到设备内部的非易失性存储器中。当日志存储空间耗尽后，需要向管理员进行告警，并提供存储空间耗尽处理机制。

4.1.10.3 日志的集中管理

SeGW应支持提供软件集中接收产生的日志。

4.1.10.4 日志统计分析和报表生成

日志软件应支持对日志进行查询、分析，并且生成报表。

4.2 性能指标

4.2.1 吞吐量

吞吐量指SeGW产品在丢包率为0的条件下网口上达到的双向数据最大流量。产品应满足用户网络环境场景对网络数据吞吐性能的要求。

4.2.2 新建隧道连接数

新建隧道连接数是指SeGW在每秒钟的时间单位内能够建立IPsec隧道数目的最大值。产品应满足用户网络环境对每秒新建隧道连接数性能的要求。

4.2.3 并发隧道连接数

并发隧道连接数是指SeGW在同一时间内能够并发的IPsec隧道数目的最大值。产品应满足用户网络环境对并发隧道连接数性能的要求。

4.2.4 加解密时延

加解密时延指SeGW产品在丢包率为0的条件下，一个明文数据流经加密变为密文，再由密文解密还原为明文所消耗的平均时间。产品应满足用户网络环境对网络数据加解密时延性能的要求。

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] RFC1631:IP网络地址转换

[10] RFFC2663:IPNAT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 无线网络安全网关技术要求
YD/T 2853—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

*
开本：880×1230　1/16　　2015 年 12 月第 1 版
印张：1　　2015 年 12 月北京第 1 次印刷
字数：20 千字
15115・737
定价：10 元
本书如有印装质量问题，请与本社联系　电话：(010)81055492