ICS 33.050
CCS M 30

团　体　标　准

T/TAF 099-2021

政企网关设备安全技术要求

Security technical requirements for enterprise gateway devices

2021-11-17 发布　　2021-11-17 实施

电信终端产业协会　发布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 安全技术要求 3
5.1 防火墙功能 3
5.2 VPN 功能 3
5.3 VxLAN 功能 4
5.4 IPv4 防攻击 4
5.5 IPv6 防攻击 4
5.6 防 ARP 攻击 4
5.7 日志功能 4
附录 A（资料性）政企网关设备典型应用场景介绍 6

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件中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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中兴通讯股份有限公司、中国信息通信研究院、新华三技术有限公司、杭州迪普科技股份有限公司、华为技术有限公司。

本文件主要起草人：刘鑫、张治兵、周继华、张亚薇、童天予、仇俊杰、叶郁柏、陈鹏、万晓兰。

引　　言

随着《网络安全法》及一系列配套政策法规的逐步落地实施，国内政企机构对网络安全的重视程度也日益提高，政企网关是部署在企业边缘网络并提供企业网络和电信网络互联的设备，政企网关自身可实现防火墙、VPN互联等业务功能。近年来全球范围内网络安全事件日益增加，政企网关安全风险也不断增加。本项目拟建立政企网关设备安全技术要求标准，提出相关安全要求，为保障和提升政企网关设备安全能力提供标准支撑。

政企网关设备安全技术要求

1 范围

本文件规定了政企网关设备在防火墙功能、VPN 功能、VxLAN 功能、IPv4 防攻击、IPv6 防攻击、防 ARP 攻击、日志功能方面的安全技术要求。本文件适用于政企网关设备的设计和生产厂商、系统集成商、设备使用方、安全检测和安全认证机构使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069-2010 信息安全技术 术语

RFC 3145 L2TP断链原因信息（L2TP Disconnect Cause Information）

RFC 3193 L2TP over IPSec（Securing L2TP using IPsec）

RFC 3931 L2TP协议3.0版本（Layer Two Tunneling Protocol - Version 3 (L2TPv3)）

RFC 3972 地址加密生成（Cryptographically Generated Addresses (CGA)）

3 术语和定义

GB/T 25069-2010中界定的以及下列术语和定义适用于本文件。

3.1

政企网关设备 enterprise gateway devices

政企网关是部署在企业边缘网络并提供企业网络和电信网络互联的设备，政企网关自身可实现防火墙、VPN 互联等业务功能。政企网关的典型应用场景见附录 A。

3.2

访问控制 access control

选择性地限制对地址空间或其他资源的访问以实现对系统资源的安全保护。

3.3

传输模式 transfer mode

传输模式是 IPSec 的一种封装方式，其保护原始 IP 头部后面的数据，在原始 IP 头和 payload 间插入 IPSec 头部。

3.4

隧道模式 tunnel mode

隧道模式是 IPSec 的一种封装方式，其保护所有 IP 数据并在 IPSec 头部前封装新的 IP 头，不使用原始 IP 头部进行路由。

3.5

邻居发现协议 neighbor discovery protocol

工作在 IPv6 网络层，负载在链路上发现其他节点和相应的地址，并确定可用路由和维护关于可用路径和其他活动节点的信息可达性。

3.6

广播风暴 broadcast storm

指当广播数据充斥网络无法处理并占用大量网络带宽，导致正常业务不能运行甚至彻底瘫痪，这就发生了“广播风暴”。

4 缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）
CHAP：挑战握手身份认证协议（Challenge Handshake Authentication Protocol）
DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）
DNS：域名系统（Domain Name System）
DoS：拒绝服务（Denial of Service）
FTP：文件传送协议（File Transfer Protocol）
HTTP：超文本传输协议（Hypertext Transfer Protocol）
HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）
ICMP: 因特网控制消息协议（Internet Control Message Protocol）
IKE：因特网密钥交换（Internet Key Exchange）
IP：因特网协议（Internet Protocol）
IPSec：互联网络层安全协议（Internet Protocol Security）
L2TP：二层隧道协议（Layer 2 Tunneling Protocol）
MAC：介质访问控制（Medium Access Control）
NTP：网络时间协议（Network Time Protocol）
POP3：邮局协议版本3（Post Office Protocol - Version 3）
RADIUS：远程用户拨号认证系统（Remote Authentication Dial In User Service）
RTSP：实时流协议（Real-time Streaming Protocol）
SIP：会话初始协议（Session Initiation Protocol）
SMTP：简单邮件传送协议（Simple Mail Transfer Protocol）
SNMP：简单网络管理协议（Simple Network Management Protocol）
TCP：传输控制协议（Transmission Control Protocol）
UDP：用户数据报协议（User Datagram Protocol）
VPN：虚拟专用网（Virtual Private Network）

VxLAN：虚拟可扩展局域网（Virtual x Local Area Network）

5 安全技术要求

5.1 防火墙功能

5.1.1 访问控制功能

a) 应支持对常用协议端口（如 80、8080、21、23 等）的开启、关闭操作。
b) 应支持基于源 MAC/IP 地址、时间段等参数实现相应的访问控制策略。
c) 应支持绑定 MAC/IP 地址功能。
d) 应支持对 IPv6 的 TC（Traffic Class，通信分类）域等参数实现相应的访问控制策略。

5.1.2 内容过滤

a) 应支持基于 URL（Uniform Resource Locator，统一资源定位）关键字的过滤功能。
b) 应支持设置黑白名单功能。
c) 可支持基于文件类型（如.doc，.xls 文件等）进行过滤。
d) 可支持针对 ActiveX、Java、Cookies、Javascript、CGI（Common Gateway Interface）、ASP（Active Server Pages）等类型的脚本程序进行过滤，具备向管理用户浏览器报警功能。

5.1.3 转发过滤

a) 应支持根据源 IP 地址及范围段、目的 IP 地址及范围段进行报文过滤。
b) 应支持根据 IP 源端口及范围段、目的端口及范围段进行报文过滤。
c) 应支持根据 IP 包的传输层协议类型进行报文过滤，并至少具有 TCP/UDP/ICMP 的选项。
d) 应支持对匹配规则的报文进行处理模式的选择，默认为禁止模式。
e) 应支持根据 TOS（Type of Service，服务类型）/DSCP（Differentiated Services Codepoint，差分服务编码点）字段对报文进行过滤的功能。
f) 宜支持协议状态检测防火墙功能，可支持对 ICMP、HTTP、HTTPS、FTP、SMTP、POP3、DNS、RADIUS、SIP、NTP、H.323、SNMP、RTSP 等协议的状态检测。

5.2 VPN 功能

政企网关设备应至少支持L2TP、IPSec、SSL VPN其中一种VPN功能。

5.2.1 L2TP

a) 应支持 LAC（L2TP Access Concentrator，L2TP 访问集中器），符合 RFC 3145 规定。
b) 应支持 CHAP 方式的隧道认证。
c) 应支持 LNS（L2TP Network Server，L2TP 网络服务器）侧本端 CHAP 认证。
d) 应支持结合 IPSec 加密的 L2TP 隧道，符合 RFC 3193 规定。
e) 宜支持 AVP（Attribute Value Pair，属性值对）隐藏传输功能。
f) 宜支持 L2TPv3，符合 RFC 3931 规定。

5.2.2 IPSec

a) 应支持 ESP(Encapsulating secutiy payload)或者 AH(Authentication header)+ESP 模式。

b) 应支持传输模式和隧道模式。
c) 应支持预共享密钥方式和 X.509 数字证书等认证方式来进行 VPN 认证。
d) 应支持通过 IKE 进行密钥交换。
e) 应支持主模式协商方式。
f) 应支持 PFS（Perfect Forward Secrecy，完全前向保密）功能（IKE 协商第二阶段）。
g) 应支持 AES128/SM4 以上强度的加密算法。支持多种哈希验证算法（SHA-256 或 SM3 等）。
h) 应支持 DPD（Dead peer detection，断线检测）协议。

5.2.3 SSL VPN

a) 应支持 TLSv1.2 及以上协议。
b) 应支持基于角色的权限管理。
c) 应支持基于用户名/密码的认证。
d) 宜支持基于证书的认证。
e) 宜支持传输层密码协议 TLCP（Transport layer cryptography protocol）。

5.3 VxLAN 功能

a) 应支持 MAC 广播限速功能。
b) 应支持 ARP 抑制功能，防止网络中出现大量 BUM（Broadcast&Unknown-unicast&Multicast）报文。
c) 应支持 VxLAN 的 MAC 表项管理功能，如 MAC 表项老化时间设置等功能。
d) 宜支持 VxLAN Over IPSec VPN 功能。

5.4 IPv4 防攻击

a) 应支持抵抗常见的 DoS 攻击。
b) 应支持防 ICMP 重定向攻击功能。
c) 宜支持 DHCP snooping 功能，减缓伪造 DHCP Server 的攻击。

5.5 IPv6 防攻击

a) 应支持抵抗常见的 DoS 攻击。
b) 应支持路由通告 RA（Router Advertisement）攻击检测功能。
c) 应支持邻居发现协议 NDP（Neighbor Discovery Protocol）攻击检测功能。
d) 宜支持安全邻居发现 SND（Secure Neighbor Discovery）协议，确保 IPv6 邻居安全可靠，符合 RFC 3972 相关规定。

5.6 防 ARP 攻击

a) 应支持 IP 地址与 MAC 地址的静态绑定来防 ARP 欺骗攻击。
b) 宜支持通过 DHCP 分配地址时自动进行 IP 地址和 MAC 地址绑定来防 ARP 欺骗攻击。
c) 应支持 ARP 广播风暴抑制功能，可设置广播报文限制的阈值。

5.7 日志功能

a) 应支持记录以下类型日志：
   1) 关键操作日志：指用户关键操作行为,例如：用户登录/注销、增/删账户、修改关键配置、重启/关闭设备等。

2) 安全事件日志：指对影响设备运行安全的事件，例如：网络攻击等。

b) 应支持日志本地存储和网络传输，且在本地存储和网络传输过程中应对日志进行保护，防止日志内容被未经授权的查看和篡改。

附 录 A
（资料性）
政企网关设备典型应用场景介绍

政企网关设备是电信运营商根据中小型企业网络场景需求所定制的网关产品，通过连接各种企业网络业务终端（包括 PC、IP 摄像头、IAD、存储设备、IT 设备、机顶盒 STB 等）为用户提供全面的企业网络业务能力。企业网络业务终端在通过政企网关实现设备互联的同时，还通过政企网关访问公众网络，并与公众网络上的业务平台和其它各类终端配合，进一步为用户提供更广泛的企业网络业务能力。

电信终端产业协会团体标准

政企网关设备安全技术要求

T/TAF 099-2021

*

版权所有 侵权必究

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn