ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 686—2018
代替 GA/T 686—2007

信息安全技术
虚拟专用网产品安全技术要求

Information security technology
Security technical requirements for virtual private network products

2018-01-26 发布　　2018-01-26 实施

中华人民共和国公安部　　发 布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GA/T 686—2007《信息安全技术　虚拟专用网安全技术要求》，与 GA/T 686—2007 相比主要变化如下：

——删除了标记的要求（见 2007 年版的 5.4）；

——删除了剩余信息保护的要求（见 2007 年版的 5.10）；

——删除了隐蔽信道分析的要求（见 2007 年版的 5.11）；

——删除了可信路径的要求（见 2007 年版的 5.12）；

——修改了标准名称；

——修改了虚拟专用网的定义（见 3.1，2007 年版的 3.1.1）；

——修改了安全保障要求（见第 8 章，2007 年版的第 6 章）；

——增加了访问控制要求（见 7.3）；

——增加了隧道建立要求（见 7.5）；

——增加了 NAT 穿越要求（见 7.6）；

——增加了 IPv6 环境适应性要求（见 7.8）；

——增加了用户的定义（见 3.4）；

——修改了等级划分要求，将等级划分为基本级和增强级两级（见 9.2、9.3，2007 年版的 A.2）。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所。

本标准主要起草人：胡维娜、李毅、赵婷、顾玮、沈亮、吴其聪。

本标准所代替标准的历次版本发布情况为：

——GA/T 686—2007。

信息安全技术
虚拟专用网产品安全技术要求

1 范围

本标准规定了虚拟专用网产品的安全功能要求、安全保障要求和等级划分要求。

本标准适用于虚拟专用网产品的设计、开发与测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 18336.3—2015 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

虚拟专用网 virtual private network

在公用网络上建立专用网络的技术。在公共的、不可信的通信基础设施上，VPN 通过设备间建立安全通信通道来保护两个通信实体间传送的数据的安全。安全通信通道通过使用加密、数字签名、鉴别、认证和访问控制等安全机制建立。

3.2

隧道 tunnel

用于传输协议的封装，在隧道的起点将待传输的原始信息经过封装处理后嵌入目标协议的数据包内，从而在支持目标协议的网络中正常传输。在隧道的终点，从封装的数据包中提取出原始信息，完成隧道两端的正常通信。

3.3

互联网协议安全 internet protocol security

由 IETF 的 IPSec 工作组提出的，将安全机制引入 TCP/IP 网络的一系列标准，是一组开放的网络安全协议的总称。IPSec 提供了完整性、认证和保密性等安全服务，主要有两种工作方式：隧道模式和传输模式。

4 缩略语

下列缩略语适用于本文件。

IETF：互联网工程任务组(Internet Engineering Task Force)

IPSec：互联网协议安全(Internet Protocol Security)

IPv6：互联网协议第六版(Internet Protocol Version 6)