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)

NAT:网络地址转换(Network Address Translation)
TCP/IP:传输控制协议/互联网协议(Transmission Control Protocol/Internet Protocol)
VPN:虚拟专用网(Virtual Private Network)

5 虚拟专用网产品描述

VPN 产品将若干个专用网络通过公共网络连接起来,使分布在不同地域的专用网络可以通过不可完全信任的公共网络(例如互联网)安全地通信。专用网络的数据经由产品建立的隧道在公共网络中传输。在 VPN 中,数据在公共网络传输的安全性应由加密技术来保障。

VPN 产品常用的工作模式有:Site-Site、Host-Site 等,图 1 是 VPN 产品典型运行环境图。

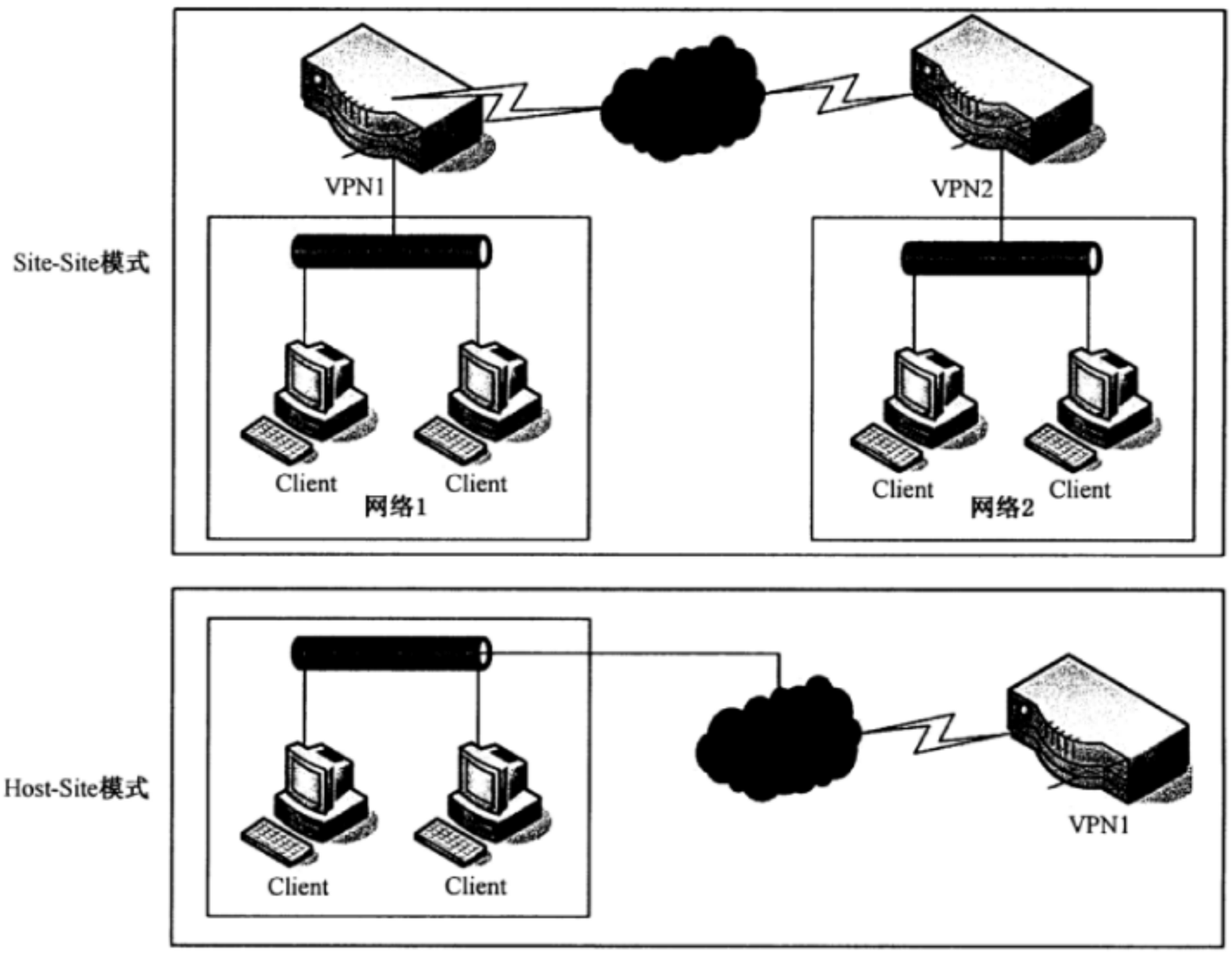

图 1 VPN 产品典型运行环境图

6 总体说明

6.1 安全技术要求分类

虚拟专用网产品安全技术要求分为安全功能和安全保障两类。其中,安全功能要求是对 VPN 产品应具备的安全功能提出具体要求,包括标识和鉴别、安全审计、访问控制、用户数据完整性保护、隧道建立、NAT 穿越、密码支持和 IPv6 环境适应性;安全保障要求针对 VPN 产品的开发和使用文档的内容提出具体的要求,例如开发、指导性文档、生命周期支持和测试等。

6.2 安全等级

按照 VPN 产品安全功能要求强度,以及按照 GB/T 18336.3—2015,对 VPN 产品安全等级进行划分。安全等级分为基本级和增强级,安全功能强弱和安全保障要求高低是等级划分的具体依据。安全

等级突出安全特性。

7 安全功能要求

7.1 标识和鉴别

7.1.1 基本标识

VPN 产品应对使用产品功能的用户进行标识。基本标识一般以用户名或用户 ID 实现。

7.1.2 唯一性标识

VPN 产品应为用户提供唯一标识，并能将标识与其所有可审计事件相关联。

7.1.3 身份鉴别

VPN 产品应保证任何用户在执行产品的安全功能前都要进行身份鉴别。应通过用户所使用设备的 MAC 地址或 IP 地址等对用户进行设备级验证。

7.1.4 鉴别失败处理

当用户鉴别失败的次数达到或超过某一给定值时，VPN 产品安全功能应：

a) 记录鉴别失败事件；
b) 终止该用户的访问；
c) 当用户是远程访问时，切断与相应主机的通信；
d) 通知 VPN 产品的安全管理员。

7.1.5 鉴别信息保护

VPN 产品应保证用户的鉴别信息以非明文方式进行存储和传输。

7.2 安全审计

7.2.1 安全审计数据产生

VPN 产品安全功能应为可审计事件生成审计记录。审计记录应包括以下内容：事件的日期和时间，事件的类型，主客体身份，事件的结果(成功或失败)。VPN 产品主要的审计事件包括：

a) 用户鉴别失败事件；
b) 授权用户的一般操作；
c) VPN 隧道的建立和删除；
d) 根据策略，数据包被丢弃事件；
e) 用户数据完整性校验失败；
f) 用户数据解密失败。

7.2.2 安全审计查阅

安全审计查阅应满足以下要求：

a) 审计查阅：为授权用户提供获得和解释审计信息的能力；
b) 有限审计查阅：禁止具有读访问权限以外的用户读取审计信息；
c) 可选审计查阅：具有根据准则来选择要查阅的审计数据的功能，并提供对审计数据进行搜索、分类、排序的能力。

7.2.3 安全审计事件存储

安全审计事件存储应满足以下要求：

a） 审计信息存储在掉电非易失性存储介质中；

b） 防止审计数据丢失：要求在审计踪迹存储记满时，应采取相应的措施防止审计数据丢失。

7.3 访问控制

若产品采用 Site-Site 模式，应支持基于源 IP、目的 IP、协议或端口、时间进行控制。

若产品采用 Host-Site 模式，应支持基于 host 端 IP、用户进行控制。

7.4 用户数据完整性保护

7.4.1 存储数据的完整性

对存储在 VPN 安全功能控制范围内的用户数据应提供完整性保护：

a） 完整性检测：要求 VPN 安全功能对存储在 VPN 内的用户数据进行完整性检测，特别是配置文件中的安全参数，应防止未授权访问和修改。可通过加密、数字签名、Hash 函数等提供存储数据的完整性保护能力。

b） 完整性检测和恢复：在检测到存储在 VPN 安全功能控制范围内用户数据的完整性错误时，要求 VPN 安全功能具有相关的恢复机制。

7.4.2 传输数据的完整性

当数据在 VPN 内传输时，VPN 设备应根据配置文件中预定的规则对数据进行完整性保护。

7.5 隧道建立

在双方提供鉴别信息后应能成功建立隧道进行数据安全传输。

7.6 NAT 穿越

若是基于 IPSec 协议的 VPN 产品应支持 NAT 穿越。

7.7 密码支持

产品使用的密码算法应符合国家密码管理的有关规定。

7.8 IPv6 环境适应性

7.8.1 纯 IPv6 环境适应性测试

产品应能够适用于纯 IPv6 环境。

7.8.2 IPv4/6 双栈环境适应性测试

产品应能够适用于 IPv4/6 双栈环境。

7.8.3 支持 IPv6 网络环境下的产品自身管理

产品组件（如果有多个组件，包括远程管理终端）间的通讯应支持 IPv6 及过渡环境。

8 安全保障要求

8.1 开发

8.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

8.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a) 完全描述产品的安全功能；
b) 描述所有安全功能接口的目的与使用方法；
c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为处理而引起的直接错误消息；
f) 证实安全功能要求到安全功能接口的追溯；
g) 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

8.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：

a) 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b) 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c) 以开发人员使用的形式提供。

8.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a) 根据子系统描述产品结构；
b) 标识和描述产品安全功能的所有子系统；
c) 描述安全功能所有子系统间的相互作用；
d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e) 根据模块描述安全功能；
f) 提供安全功能子系统到模块间的映射关系；
g) 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i) 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

8.2 指导性文档

8.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

a) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用产品提供的可用接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识产品运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；
f) 充分实现安全目的所必须执行的安全策略。

8.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

8.3 生命周期支持

8.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品，实施的配置管理与配置管理计划相一致；
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

8.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

8.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

8.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现

的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

8.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

8.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

8.4 测试

8.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；

b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

8.4.2 深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；

b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

8.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b) 预期的测试结果，表明测试成功后的预期输出；

c) 实际测试结果和预期的一致性。

8.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

8.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；

b) 具有增强型基本攻击潜力的攻击者的攻击。

9 等级划分要求

9.1 概述

VPN 产品的安全功能要求和安全保障要求划分为基本级和增强级。

9.2 安全功能要求等级划分

VPN 产品的安全功能要求等级划分如表 1 所示。

表 1　VPN 产品安全功能要求等级划分表

安全功能要求		基本级	增强级
标识和鉴别	基本标识	7.1.1	7.1.1
	唯一性标识	7.1.2	7.1.2
	身份鉴别	7.1.3	7.1.3
	鉴别失败处理	7.1.4a)～7.1.4c)	7.1.4
	鉴别信息保护	7.1.5	7.1.5
安全审计	安全审计数据产生	7.2.1a)～7.2.1d)	7.2.1
	安全审计查阅	7.2.2a)、7.2.2b)	7.2.2
	安全审计事件存储	7.2.3a)	7.2.3
访问控制		7.3	7.3
用户数据完整性保护	存储数据的完整性	—	7.4.1
	传输数据的完整性	7.4.2	7.4.2
隧道建立		7.5	7.5
NAT 穿越		7.6	7.6
密码支持		7.7	7.7
IPv6 环境适应性	纯 IPv6 环境适应性测试	—	7.8.1
	IPv4/6 双栈环境适应性测试	—	7.8.2
	支持 IPv6 网络环境下的产品自身管理	—	7.8.3

9.3　安全保障要求等级划分

VPN 产品的安全保障要求等级划分如表 2 所示。

表 2　VPN 产品安全保障要求等级划分表

安全保障要求		基本级	增强级
开发	安全架构	8.1.1	8.1.1
	功能规范	8.1.2a)～8.1.2f)	8.1.2
	实现表示	—	8.1.3
	产品设计	8.1.4a)～8.1.4d)	8.1.4
指导性文档	操作用户指南	8.2.1	8.2.1
	准备程序	8.2.2	8.2.2
生命周期支持	配置管理能力	8.3.1a)～8.3.1c)	8.3.1
	配置管理范围	8.3.2a)	8.3.2
	交付程序	8.3.3	8.3.3
	开发安全	—	8.3.4

表 2（续）

安全保障要求		基本级	增强级
生命周期支持	生命周期定义	—	8.3.5
	工具和技术	—	8.3.6
测试	覆盖	8.4.1a)	8.4.1
	深度	—	8.4.2
	功能测试	8.4.3	8.4.3
	独立测试	8.4.4	8.4.4
脆弱性评定		8.5a)	8.5b)