ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 686—2007

信息安全技术
虚拟专用网安全技术要求

Information security technology—
Technical requirements of virtual private network security

2007-03-20 发布　　2007-05-01 实施

中华人民共和国公安部　　发 布

目　　次

前言 …… Ⅴ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
4　VPN 的一般说明 …… 2
4.1　概述 …… 2
4.2　安全环境 …… 2
4.2.1　安全威胁 …… 2
4.2.2　安全应用假设 …… 3
5　安全功能技术要求 …… 3
5.1　标识和鉴别 …… 3
5.1.1　用户标识 …… 3
5.1.2　用户鉴别 …… 3
5.1.3　鉴别失败处理 …… 4
5.1.4　用户-主体绑定 …… 4
5.2　安全审计 …… 4
5.2.1　安全审计的响应 …… 4
5.2.2　安全审计数据产生 …… 4
5.2.3　安全审计分析 …… 5
5.2.4　安全审计查阅 …… 5
5.2.5　安全审计事件存储 …… 5
5.2.6　网络环境安全审计与评估 …… 5
5.3　通信抗抵赖 …… 6
5.3.1　抗原发抵赖 …… 6
5.3.2　抗接收抵赖 …… 6
5.4　标记 …… 6
5.5　自主访问控制 …… 7
5.6　强制访问控制 …… 7
5.7　用户数据存储保护 …… 7
5.8　用户数据传输保护 …… 7
5.8.1　VPN 内数据传输保护 …… 7
5.8.2　VPN 向公用网络输出数据的保护 …… 7
5.8.3　公用网络向 VPN 输入数据的保护 …… 8
5.9　用户数据完整性保护 …… 8
5.9.1　存储数据的完整性 …… 8
5.9.2　传输数据的完整性 …… 8
5.9.3　处理数据的完整性 …… 8

5.10 剩余信息保护…… 8
5.11 隐蔽信道分析…… 8
5.11.1 一般性的隐蔽信道分析…… 8
5.11.2 系统化的隐蔽信道分析…… 9
5.11.3 彻底化的隐蔽信道分析…… 9
5.12 可信路径…… 9
5.13 密码支持…… 9
6 安全保证技术要求 …… 9
6.1 VPN 安全功能自身安全保护…… 9
6.1.1 安全运行测试 …… 9
6.1.2 失败保护 …… 9
6.1.3 输出 VPN 安全功能数据的可用性 …… 9
6.1.4 输出 VPN 安全功能数据的保密性 …… 10
6.1.5 输出 VPN 安全功能数据的完整性 …… 10
6.1.6 VPN 内 VPN 安全功能数据传输 …… 10
6.1.7 物理安全保护…… 10
6.1.8 可信恢复…… 10
6.1.9 重放检测…… 11
6.1.10 参照仲裁 …… 11
6.1.11 域分离 …… 11
6.1.12 状态同步协议 …… 11
6.1.13 时间戳 …… 11
6.1.14 数据一致性 …… 11
6.1.15 安全功能检测 …… 11
6.1.16 资源利用 …… 11
6.1.17 VPN 安全设施访问控制…… 12
6.1.18 可信路径/信道…… 12
6.2 VPN 设计和实现 …… 13
6.2.1 配置管理…… 13
6.2.2 分发和操作…… 14
6.2.3 开发…… 14
6.2.4 指导性文档…… 16
6.2.5 生命周期支持…… 16
6.2.6 测试…… 17
6.2.7 脆弱性评定…… 18
6.3 VPN 安全设施安全管理 …… 19
6.3.1 功能管理…… 19
6.3.2 安全属性的管理…… 19
6.3.3 VPN 安全功能数据的管理 …… 19
6.3.4 安全角色管理…… 19
6.3.5 时限授权…… 20
6.3.6 撤销…… 20
7 VPN 安全保护等级划分要求 …… 20

7.1 第一级:用户自主保护级 …… 20
7.1.1 安全功能技术要求 …… 20
7.1.2 安全保证技术要求 …… 20
7.2 第二级:系统审计保护级 …… 21
7.2.1 安全功能技术要求 …… 21
7.2.2 安全保证技术要求 …… 22
7.3 第三级:安全标记保护级 …… 23
7.3.1 安全功能技术要求 …… 23
7.3.2 安全保证技术要求 …… 24
7.4 第四级:结构化保护级 …… 25
7.4.1 安全功能技术要求 …… 25
7.4.2 安全保证技术要求 …… 26
7.5 第五级:访问验证保护级 …… 28
7.5.1 安全功能技术要求 …… 28
7.5.2 安全保证技术要求 …… 29
附录 A(资料性附录) 标准概念说明 …… 31
A.1 组成与相互关系 …… 31
A.2 VPN 安全等级的划分 …… 31
A.3 关于 VPN 中的主体与客体 …… 33
A.4 关于 VPN 中的安全设施、安全功能和安全功能策略 …… 33
A.5 关于密码技术 …… 34
参考文献 …… 35

前　言

本标准从信息技术方面详细规定了各安全保护级别的 VPN 系统所应具有的安全功能要求和安全保证要求。

本标准的附录 A 为资料性附录。

本标准由公安部公共信息网络安全监察局提出。

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：中国科学院研究生院信息安全国家重点实验室。

本标准主要起草人：荆继武、冯登国、夏鲁宁、聂晓峰、黄敏、王琼霄、许良玉、高能、林璟锵、吕欣、廖洪銮。

引　言

本标准用以指导设计者如何设计和实现具有所需要的安全等级的虚拟专用网产品，主要从对虚拟专用网的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现 GB 17859—1999 中每一个安全保护等级的安全要求对虚拟专用网应采取的安全技术措施，以及各安全技术要求在不同安全保护等级中具体实现上的差异。

本标准对虚拟专用网系统安全等级保护所涉及的安全功能技术要求和安全保证技术要求做了比较全面的描述，按 GB 17859—1999 五个安全保护等级的划分，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。文中每一级别比上一级别新增的要求以加粗字表示。

信息安全技术
虚拟专用网安全技术要求

1 范围

本标准规定了按 GB 17859—1999 对虚拟专用网进行安全等级保护划分所需要的详细技术要求。

本标准适用于按 GB 17859—1999 的安全等级保护要求所进行的虚拟专用网的设计和实现。按 GB 17859—1999安全等级保护的要求对虚拟专用网进行的测试、管理也可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是标注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 18336.1—2001　信息技术　安全技术　信息技术安全性评估准则　第1部分：简介和一般模型

3 术语、定义和缩略语

3.1 术语和定义

GB 17859—1999 和 GB/T 18336.1—2001 确立的以及下列术语、定义适用于本标准。

3.1.1

虚拟专用网　virtual private network；VPN

虚拟专用网，又称虚拟私人网络。VPN 是一门网络技术，它为我们提供了一种像使用安全专用网络一样使用公用网络(例如互联网)的能力。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。安全通信通道可以建立在局域网、城域网、私有广域网和公用广域网(例如互联网)之上。

3.1.2

VPN 安全设施　trusted computing base(TCB) of VPN

在 VPN 中，VPN 安全设施是 VPN 中保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立一个基本的保护环境，并提供 VPN 所要求的附加服务。VPN 中，VPN 安全设施是一个物理上分散，逻辑上统一的分布式安全设施。

3.1.3

VPN 安全功能策略　TCB security function policy of VPN

对 VPN 安全设施中的资源进行管理、保护和分配的一组规则。VPN 安全功能策略构成一个安全域，以防止不可信主体的干扰和篡改。一个 VPN 安全设施可以有一个或多个安全功能策略。

3.1.4

VPN 安全功能　TCB security function of VPN

正确实施 VPN 安全功能策略的全部硬件、固件、软件所提供的功能。每一个安全功能策略的实现，组成一个安全功能模块。一个 VPN 安全设施的所有安全功能模块共同组成该 VPN 安全设施的安