ICS 35.040
L 80
备案号:44624—2014

GM

中华人民共和国密码行业标准

GM/T 0023—2014

IPSec VPN 网关产品规范

IPSec VPN gateway product specification

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
IPSec VPN 网关产品规范
GM/T 0023—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)64275323　发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.25　字数 30 千字
2014 年 4 月第一版　2014 年 4 月第一次印刷
*
书号:155066·2-27009　定价 23.00 元

GM/T 0023-2014

目　　次

前　言

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。

本标准由密码行业标准化技术委员会提出并归口。

本标准主要起草单位：成都卫士通信息产业股份有限公司、上海格尔软件股份有限公司、无锡江南信息安全工程技术中心、兴唐通信科技有限公司、山东得安计算机技术有限公司。

本标准主要起草人：罗俊、李元正、谭武征、徐强、王妮娜、孔凡玉。

IPSec VPN 网关产品规范

1 范围

本标准规定了 IPSec VPN 网关产品的功能要求、硬件要求、软件要求、密码算法和密钥要求、安全性要求和检测要求等有关内容。

本标准适用于 IPSec VPN 网关产品的研制、检测、使用和管理。

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 2423—2008 电工电子产品环境试验(所有部分)

GB/T 9813—2000 微型计算机通用规范

GB/T 15153.1—1998 远动设备及系统 第 2 部分：工作条件 第 1 篇：电源和电磁兼容性

GB/T 17964—2008 信息安全技术 分组密码算法的工作模式

GM/T 0005 随机性检测规范

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0022 IPSec VPN 技术规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

密码算法 cryptographic algorithm

描述密码处理过程的运算规则。

3.1.2

密码杂凑算法 cryptographic hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

a) 为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

b) 为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

c) 要发现不同的输入映射到同一输出是计算上困难的。

3.1.3

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开，另一个密钥(私钥)必须保密，且由公钥求解私钥是计算不可行的。

3.1.4

对称密码算法　symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.1.5

分组密码算法　block cipher algorithm

将输入数据划分成固定长度的分组进行加解密的一类对称密码算法。

3.1.6

SM1 算法　SM1 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.1.7

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

3.1.8

SM3 算法　SM3 algorithm

一种密码杂凑算法，其输出为 256 比特。

3.1.9

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.1.10

密文分组链接工作模式　cipher block chaining operation mode；CBC

分组密码算法的一种工作模式，其特征是将当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前的密文分组。

3.1.11

初始化向量/值　initialization vector/initialization value；IV

在密码变换中，为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

3.1.12

数据源鉴别　data origin authentication

对数据的来源或发送方进行鉴别，确认接收到的数据的来源是所声称的。

3.1.13

数字证书　digital certificate

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.1.14

IPSec 协议　internet protocol security

一种端到端的确保基于 IP 通信数据安全性的网络层协议，可以提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

3.1.15

安全联盟　security association；SA

两个通信实体经协商建立起来的一种协定，它描述了实体如何利用安全服务来进行安全的通信。安全联盟包括了执行各种网络安全服务所需要的所有信息，例如 IP 层服务(如头鉴别和载荷封装)、传输层和应用层服务或者协商通信的自我保护。

3.1.16

鉴别头　authentication header；AH

属于 IPSec 的一种协议，用于提供 IP 数据包的数据完整性、数据源鉴别以及抗重放攻击的功能，但不提供数据机密性的功能。

3.1.17

封装安全载荷　encapsulating security payload；ESP

属于 IPSec 的一种协议，用于提供 IP 数据包的机密性、数据完整性以及对数据源鉴别以及抗重放攻击的功能。

3.1.18

虚拟专用网　virtual private network；VPN

使用密码技术在通信网络中构建安全通道的技术。

3.2　缩略语

下列缩略语适用于本文件。

AH：鉴别头（Authentication Header）

CBC：密码分组链接工作模式（Cipher Block Chaining）

ESP：封装安全载荷（Encapsulating Security Payload）

HMAC：带密钥的杂凑算法（Keyed-HASH Message Authentication Code）

IPSec：IP 安全协议（Internet Protocol Security）

IV：初始化向量（Initialization Vecto）

NAT：网络地址转换（Network Address Translation）

SA：安全联盟（Security Association）

VPN：虚拟专用网络（Virtual Private Network）

4　密码算法和密钥种类

4.1　算法要求

IPSec VPN 使用国家密码管理主管部门批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法。算法使用要求如下：

——非对称密码算法用于鉴别、数字签名和数字信封等。

——对称密码算法使用分组密码算法，用于密钥交换数据的加密保护和报文数据的加密保护。算法的工作模式使用 CBC 模式，应符合 GB/T 17964—2008 的要求。

——密码杂凑算法用于对称密钥生成和完整性校验。

——生成的随机数应能通过 GM/T 0005 的检测。

4.2　密钥种类

IPSec VPN 使用下列密钥：

——设备密钥：非对称算法使用的公私钥对，包括签名密钥对和加密密钥对，其中签名密钥对用于鉴别和数字签名，加密密钥对用于数字信封。

——工作密钥：在密钥交换第一阶段得到的对称算法密钥，用于保护会话密钥交换的过程。

——会话密钥：在密钥交换第二阶段得到的对称算法密钥，用于数据报文的加密和完整性保护。

5 IPSec VPN 网关产品要求

5.1 产品功能要求

5.1.1 随机数生成

IPSec VPN 网关产品应具有随机数生成功能，其随机数应由多路硬件噪声源产生。

5.1.2 工作模式

IPSec VPN 网关产品工作模式应支持隧道模式和传输模式，其中隧道模式是必备功能，用于主机和网关实现，传输模式是可选功能，仅用于主机实现。

5.1.3 密钥交换

IPSec VPN 网关产品应具有密钥交换功能，通过协商产生工作密钥和会话密钥。

密钥交换协议应按照 GM/T 0022 中 5.1 的要求进行。

IPSec VPN 网关产品开机后应重新发起密钥交换。

5.1.4 安全报文封装

安全报文封装协议分为 AH 协议和 ESP 协议。

AH 协议应与 ESP 协议嵌套使用，这种情况下不启用 ESP 协议中的验证操作。

ESP 协议可单独使用，这种情况下应启用 ESP 协议中的验证操作。

安全报文封装协议应符合 GM/T 0022 中 5.2 的要求。

5.1.5 NAT 穿越

IPSec VPN 网关产品应支持 ESP 单独使用时 NAT 穿越。

NAT 穿越协议应符合 GM/T 0022 中 5.1.3 的要求。

5.1.6 鉴别方式

IPSec VPN 网关产品应具有实体鉴别的功能，鉴别方式应采用数字证书。数字证书格式应满足 GM/T 0015 的要求。

5.1.7 IP 协议版本支持

IPSec VPN 网关产品支持 IPv4 协议，可选支持 IPv6 协议。

5.1.8 抗重放攻击

IPSec VPN 网关产品在安全报文传输阶段应具有对抗重放攻击的功能。

5.1.9 密钥更新

IPSec VPN 网关产品应具有根据时间周期和报文流量两种条件进行工作密钥和会话密钥的更新功能，其中根据时间周期条件进行密钥更新为必备功能，根据报文流量条件进行密钥更新为可选功能。

工作密钥的最大更新周期不大于 24 h。如果采用流量条件，最大更新流量不大于 2^{10}（按每报文 1024 字节计算）×2^{32}（对应于 32 比特的抗重放序列号）字节。

会话密钥的最大更新周期不大于 1 h。如果采用流量条件，最大更新流量不大于 2^{10}（按每报文

1024 字节计算)×2^{32}(对应于 32 比特的抗重放序列号)字节。

5.1.10 包过滤

IPSec VPN 网关产品应具有根据数据报文的五元组(源 IP 地址、目的 IP 地址、源传输层端口、目的传输层端口、传输层协议)决定其处理方式的功能。处理方式需要支持丢弃、明文转发(绕过 IPSec 处理)、密文转发(使用 IPSec 处理后转发)等。

5.2 产品性能参数

5.2.1 加解密吞吐率

加解密吞吐率是指分别在 64 字节以太帧长和 1428(IPv4)/1408(IPv6)字节以太帧长时,IPSec VPN网关产品在丢包率为 0 的条件下内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对网络数据加解密吞吐性能的要求。

5.2.2 加解密时延

加解密时延是指分别在 64 字节以太帧长和 1428(IPv4)/1408(IPv6)字节以太帧长时,IPSec VPN网关产品在丢包率为 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。

5.2.3 加解密丢包率

加解密丢包率是指分别在 64 字节以太帧长和 1428(IPv4)/1408(IPv6)字节以太帧长时,在IPSec VPN网关产品内网口处于线速情况下,单位时间内错误或丢失的数据包占总发数据包数量的百分比。产品应满足用户网络环境对网络数据加解密丢包率性能的要求。

5.2.4 每秒新建隧道数

每秒新建隧道数是指 IPSec VPN 网关产品在一秒钟的时间单位内能够新建立隧道数目的最大值。产品应满足用户网络环境对每秒新建隧道数性能的要求。

5.2.5 最大并发隧道数

最大并发隧道数是指 IPSec VPN 网关产品同时并存的隧道数目的最大值。产品应满足用户网络环境对最大并发隧道数性能的要求。

5.3 安全性要求

5.3.1 密钥安全

5.3.1.1 设备密钥

IPSec VPN 网关产品的设备密钥是非对称密钥,包括签名密钥对和加密密钥对。

签名密钥对由 IPSec VPN 产品自身产生,其公钥应能被导出,由外部认证机构签发签名证书。

加密密钥对由外部密钥管理机构产生并由外部认证机构签发加密证书。加密密钥对的私钥保护方法见 GM/T 0014。

签名证书、加密证书和加密密钥对的私钥应能被导入 IPSec VPN 产品中。

在 IPSec VPN 产品中,设备密钥的私钥应有安全保护措施。

设备密钥应按设定的安全策略进行更新。

设备密钥可以安全形式进行备份，并在需要时能够恢复。

5.3.1.2 工作密钥

工作密钥在密钥交换的第一阶段产生，产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

5.3.1.3 会话密钥

会话密钥在密钥交换的第二阶段产生，产生后应保存在易失性存储器中，达到其更新条件后应立即更换，在连接断开、设备断电时应销毁。

5.3.2 硬件安全

IPSec VPN 网关产品应提供安全措施，保证密码算法、密钥、关键数据的存储安全。

所有密码运算应在独立的密码部件中进行。

除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。远程维护接口应采用加密通道和身份鉴别等安全措施。

5.3.3 软件安全

所有的安全协议及管理软件应自主实现。源代码完全可控。

操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。

任何操作指令及其任意组合，不能泄露密钥和敏感信息。

5.4 管理功能要求

5.4.1 合规性验证

5.4.1.1 对称算法验证

IPSec VPN 网关产品可提供远程调用接口接受国家密码管理主管部门对其 SM1 和 SM4 对称加密算法进行合规性验证。验证协议和接口应符合国家密码管理主管部门的要求。

5.4.1.2 非对称算法验证

IPSec VPN 网关产品可提供远程调用接口接受国家密码管理主管部门对其 SM2 非对称加密算法合规性进行验证。验证协议和接口应符合国家密码管理主管部门的要求。

5.4.1.3 杂凑算法验证

IPSec VPN 网关产品可提供远程调用接口接受国家密码管理主管部门对其 SM3 杂凑算法合规性进行验证。验证协议和接口应符合国家密码管理主管部门的要求。

5.4.1.4 密钥随机性验证

IPSec VPN 网关产品可提供远程调用接口接受国家密码管理主管部门对其密钥随机性进行验证。验证协议和接口应符合国家密码管理主管部门的要求。

5.4.2 参数配置管理

5.4.2.1 安全策略配置

IP 数据报文的源 IP 地址（或子网、地址范围）、目的 IP 地址（或子网、地址范围）、协议类型

(TCP/UDP/ICMP/ALL)、源端口地址和目的端口地址(针对 TCP 和 UDP)或 ICMP 请求类型构成一个五元组(五元组标志定义详见 GM/T 0022),加上对匹配该五元组的处理方式:丢弃、绕过 IPSec 处理或采用 IPSec 处理及该处理对应的 SA 安全联盟(见 GM/T 0022)构成一条 IPSec 安全策略,IPSec VPN网关产品可提供协议和接口接受管理中心对其 IPSec 安全策略进行修改、添加、删除等操作。

5.4.2.2 安全参数配置

IPSec VPN 网关产品可提供协议和接口接受管理中心对其安全参数进行配置,可配置参数包括 SA 安全联盟(见 GM/T 0022)的算法套件和用于隧道封装的 IP 地址、密钥更新时间或流量、访问控制地址和端口列表(白名单或黑名单)、访问控制时间段和资源列表等,可对以上参数进行修改、添加、删除等操作。

5.4.2.3 网络参数配置

IPSec VPN 网关产品可提供协议和接口接受管理中心对其网络配置参数进行设置,可配置参数包括网络接口 IP 地址、MAC 绑定、主机和子网路由、缺省网关地址、网桥与生成树相关参数、域名等,可对以上参数进行修改、添加、删除等操作。

5.4.2.4 用户参数配置

当支持客户端模式时,IPSec VPN 网关产品可提供协议和接口接受管理中心对其用户信息进行设置,包括用户名和口令、用户配置信息(接入用 IP 地址、网关 IP 地址、DNS 服务器地址等)、用户有效期等,可对以上参数进行修改、添加、删除等操作。

5.4.2.5 其他参数配置

IPSec VPN 网关产品可提供协议和接口接受管理中心对其其他功能模块的参数进行设置。

5.4.3 远程监控管理

5.4.3.1 参数查询

IPSec VPN 网关产品可提供协议和接口接受管理中心对其安全策略、安全参数、网络参数、用户参数等配置信息和日志进行查询,并可提供分类查询和关键字检索手段。

5.4.3.2 状态监测

IPSec VPN 网关产品可提供协议和接口接受管理中心对其运行状态(CPU、内存和非易失性存储介质等系统资源的占有率)、系统信息(开机时间、运行时间、系统时间和设备名字及 IP 等)、网络流量、是否在线、隧道状态(建立时间、加密流量、有效期等)进行远程实时查询,并在设备状态明显异常时可向管理中心报警。

5.4.3.3 远程控制

IPSec VPN 网关产品可提供协议和接口接受管理中心对其进行重启、故障诊断、各项功能的关闭和启用等操作。

5.4.3.4 时间同步

IPSec VPN 网关产品可提供远程调用接口接受管理中心对其进行远程时间同步。

5.4.4 日志管理

IPSec VPN 网关产品应提供日志功能，日志可被查看、导出。日志的记录要素必须包括事件发生的日期、时间、主体、客体、类型和结果等。

日志内容包括：

——操作行为，包括登录鉴别、参数配置、策略配置、密钥管理等操作；

——安全事件，密钥交换成功及失败、密钥过期、隧道建立及删除等事件；

——异常事件，解密失败、完整性校验失败等异常事件的统计。

5.4.5 管理员管理

IPSec VPN 网关产品应设置管理员，并实现系统管理员、安全管理员、审计管理员分权管理。安全管理员负责设备参数配置、策略配置、设备密钥的生成、导入、备份和恢复等操作。系统管理员负责对软件环境日常运行的管理和维护，对管理员的管理和权限分配，以及对系统的备份和恢复。审计管理员负责对系统中的日志进行安全审计。

管理员应持有表征用户身份信息的硬件装置和数字证书，与登录口令相结合并通过加密通道登录系统，进行管理操作前应通过身份鉴别。

管理员只能通过被授权的终端登录到 IPSec VPN 网关进行相应的配置操作。

登录口令长度应不小于 8 个字符，应不包含全部或部分用户账号名，并至少包含以下四类字符中的三类：大写字母、小写字母、数字、键盘上的符号。

使用错误口令或非法身份登录的次数限制应小于或等于 8。

5.4.6 设备管理

5.4.6.1 设备初始化

IPSec VPN 网关产品的初始化，除必须由厂商进行的操作外，参数的配置、安全策略的配置、密钥的生成和管理、管理员的产生等均应由用户完成。初始化数据中如含有私钥等敏感信息应提供安全 IC 卡或安全 Key 等硬件介质承载。

5.4.6.2 设备注册

IPSec VPN 网关产品可具有向管理中心进行自动注册的功能，注册过程应按照国家密码管理机构的要求进行。

5.4.6.3 设备自检

IPSec VPN 网关产品每次启动时均应该进行自检。

应对密码运算部件等关键部件进行正确性检查。应确保密码运算部件正常工作，设备所采用的各种密码算法：包括对称、杂凑和非对称算法的正确性在设备自检时应得到验证。

应对存储的密钥等敏感信息进行完整性检查。应确保设备密钥得到安全保护，工作密钥和会话密钥不存放在非易失性存储介质中。

应对硬件随机数产生部件进行检查，应确保硬件随机数产生部件正常工作，随机数产生质量符合规定。

应对身份鉴别介质及其接口进行检查，确保其正常工作。

可对 CPU、内存、网络接口、非易失性存储介质等物理部件进行常规检查，确保各关键部件正常工作。

在检查不通过时应报警并停止工作。

5.4.7 远程管理

IPSec VPN 网关产品可提供协议和接口接受管理中心通过安全网络通道对其进行算法等合规性验证和设备参数与状态等的查询和设置，协议和接口应符合国家密码管理主管部门的要求。

5.5 硬件要求

5.5.1 对外接口

IPSec VPN 网关产品应至少具备两个工作网口，支持双臂（即具备两个网络接口，采用串接的方式将设备接入网络）接入，可选支持单臂接入（以单个网络接口用旁路的方式将设备接入网络）。还应提供一个管理接口，可以通过 TCP/IP 网络或串行接口与管理设备连接。

5.5.2 加密部件

IPSec VPN 网关产品应采用经过国家密码管理主管部门审批的加密芯片或加密卡作为主要加密部件。

5.5.3 随机数发生器

IPSec VPN 网关产品的随机数发生器采用国家密码管理主管部门批准的物理噪声源，应提供多路随机源，至少采用两个独立的物理噪声源芯片实现。

IPSec VPN 网关产品应提供随机数采集接口。随机数发生器能通过送样检测、出厂检测、上电检测和使用检测四个不同应用阶段的随机数检测：

a) 送样检测

依据 GM/T 0005 进行随机数检测。

b) 出厂检测

- 检测量：采集 50×10^6 比特随机数，分成 50 组，每组 10^6 比特；
- 检测项目：依据 GM/T 0005 进行检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格；

允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

c) 上电检测

- 检测量：采集 20×10^6 比特随机数，分成 20 组，每组 10^6 比特；
- 检测项目：依据 GM/T 0005 进行检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。

允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

d) 使用检测

1) 周期检测

- 检测量：采集 4×10^5 比特随机数，分成 20 组，每组 20000 比特；
- 检测项目：对采集随机数按照 GM/T 0005 中除离散傅立叶检测、线性复杂度检测、通用统计检测外的 12 项项目检测；
- 检测通过标准：检测中如果有一项不通过检测标准，则告警检测不合格。允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效；
- 检测周期：可配置，检测间隔最长不超过 12 h。

2） 单次检测

- 检测量：根据实际应用时每次所采随机数大小确定，但长度不应低于 128 比特，且已通过检测的未用序列可继续用；
- 检测项目：扑克检测。当样本长度小于 320 比特时，参数 $m=2$；

检测通过标准：检测中如果不通过检测标准，则告警检测不合格。

允许重复 1 次随机数采集与检测，如果重复检测仍不合格，则判定为产品的随机数发生器失效。

5.5.4 环境适应性

IPSec VPN 网关产品的工作环境应根据实际需要遵循 GB/T 9813—2000 中关于“气候环境适应性”的规定要求。

5.5.5 电磁兼容性

IPSec VPN 网关产品应满足一定条件下的电磁兼容等级，见 GB/T 15153.1—1998 对电磁兼容性的要求。

5.5.6 可靠性

IPSec VPN 网关产品的平均无故障工作时间应不低于 10000 h，平均可持续加密流量应不低于 10000 Gb，可采用双机热备和负载均衡等部署方式提高可靠性。

5.6 参数可配置能力要求

IPSec VPN 网关产品可支持对设备的相关参数进行配置，包括网络接口的 MTU（最大传输单元）、MAC 地址、速度（自适应或者固定速率）、双工/半双工、是否开启流控等。

5.7 过程保护

设置必要保护措施，保障产品在运输和安装过程中的安全，不被嵌入恶意信息。

6 IPSec VPN 网关产品检测

6.1 产品功能检测

6.1.1 随机数生成

按照 GM/T 0005 的要求提取样本，并按照该规范的相关要求进行检测，检测结果应符合 5.1.1 的要求。

6.1.2 工作模式

将检测设备与被测设备均设置为隧道模式，应能成功完成密钥交换，建立 IPSec 隧道进行通信。

被测设备支持传输模式时，将检测设备与被测设备均设置为传输模式，应能成功完成密钥交换，进行通信。

将检测设备与被测设备一方设置为隧道模式，另一方设置为传输模式，密钥交换应失败，无法建立 IPSec 隧道进行通信。

6.1.3 密钥交换

按 GM/T 0022 中 5.1.2 的方法进行密钥交换。将检测设备与被测设备配置相同算法套件、封装协议和工作模式，应能成功完成密钥交换并建立 IPSec 隧道。对密钥交换过程进行网络数据截获，查看其过程应符合 GM/T 0022 中 5.1.2 的要求，其报文格式应符合 GM/T 0022 中 5.1.4 的要求。

6.1.4 安全报文封装协议

将检测设备与被测设备的安全报文封装协议均配置为隧道模式的 ESP 协议，应能成功完成密钥交换，建立 IPSec 隧道并正确进行加密通信。对加密通信的报文进行网络数据截获，查看其封装格式应符合 GM/T 0022 中 5.2.2 的要求。

将检测设备与被测设备的安全报文封装协议均配置为隧道模式的 AH 协议嵌套 ESP 协议，应能成功完成密钥交换，建立 IPSec 隧道并正确进行加密通信。对加密通信的报文进行网络数据截获，查看其封装格式应符合 GM/T 0022 中 5.2.1 和 5.2.2 的要求。

6.1.5 NAT 穿越

将待检测设备放在 NAT 下，按 GM/T 0022 中 5.1.3 的方法进行密钥交换，将检测设备与被测设备配置相同算法套件、封装协议和工作模式，应能成功完成密钥交换并建立 IPSec 隧道。对密钥交换过程进行网络数据截获，查看其过程应符合 GM/T 0022 中 5.1.3 的要求，其报文格式应符合 GM/T 0022 中 5.1.4 的要求。

将检测设备与被测设备的安全报文封装协议均配置为隧道模式的 ESP 协议，应能成功完成密钥交换，建立 IPSec 隧道并正确进行加密通信。对加密通信的报文进行网络数据截获，查看其封装格式应符合 GM/T 0022 中 5.2.3(RFC 3948)的要求。

6.1.6 鉴别方式

按产品提供的鉴别方式，按 GM/T 0022 中 5.1.2 的方法进行密钥交换，应能成功完成交换过程，建立 IPSec 隧道进行通信。

6.1.7 IP 协议版本支持

在 IPv4 或者 IPv6 的环境下，按 GM/T 0022 中 5.1.2 的方法进行密钥交换，应能成功完成交换过程，建立 IPSec 隧道进行通信。

6.1.8 抗重放攻击

利用测试设备或网络报文截获工具重放报文传输阶段的安全报文，在被测设备的内网口应不能检测到重放的数据报文。

6.1.9 密钥更新

在检测设备和被测设备上按照相同参数设定工作密钥和会话密钥的更新周期，应能成功完成密钥的更新。当满足更新条件时，使用网络报文截获工具应能分别看到相应的第一阶段和第二阶段的密钥交换过程。

如果设备具有根据流量更新密钥的功能，在检测设备和被测设备上按照相同参数设定会话密钥的流量更新条件，应能成功完成密钥的更新。当满足更新条件时，使用网络报文截获工具应能看到第二阶段的密钥交换过程。

6.1.10 包过滤

在被测设备上分别配置不同五元组对应 IPSec 策略(见 5.4.2.1)的处理选择为丢弃、绕过 IPSec 或使用 IPSec 处理,利用测试设备在被测设备的内网口发送不同五元组的数据报文,在被测设备的外网口应不能检测到设定为丢弃的数据报文、可检测到设定为绕过 IPSec 的数据报文明文、可检测到设定为使用 IPSec 处理的数据报文密文。

6.2 产品性能检测

6.2.1 加解密吞吐率

根据 5.2.1 加解密吞吐率的定义,将网关产品连接检测平台进行检测。

6.2.2 加解密时延

根据 5.2.2 加解密时延的定义,将网关产品连接检测平台进行检测。

6.2.3 加解密丢包率

根据 5.2.3 加解密丢包率的定义,将网关产品连接检测平台进行检测。

6.2.4 每秒新建隧道数

根据 5.2.4,将网关产品连接检测平台进行检测。

6.2.5 最大并发隧道数

根据 5.2.5,将网关产品连接检测平台进行检测。

6.3 安全性检测

6.3.1 密钥安全

6.3.1.1 设备密钥安全

在被测设备的管理界面上进行设备密钥的产生或导入、备份和恢复以及更新操作。检测结果应符合 5.3.1.1 的要求。

6.3.1.2 工作密钥安全

检测结果应符合 5.3.1.2 的要求。

6.3.1.3 会话密钥安全

检测结果应符合 5.3.1.3 的要求。

6.3.2 硬件安全

审查厂商提供的设计文档和厂商提交的产品安全性承诺,应符合 5.3.2 的要求。

6.3.3 软件安全

使用扫描工具探测系统的端口和服务,并审查厂商提供的设计文档和厂商提交的产品安全性承诺,应符合 5.3.3 的要求。

6.4 管理功能检测

6.4.1 合规性验证

进行设备的合规性验证等管理操作，结果应符合 5.4.1 的要求。

6.4.2 参数配置管理

进行设备的参数配置等管理操作，结果应符合 5.4.2 的要求。

6.4.3 远程监控管理

进行设备的远程监控等管理操作，结果应符合 5.4.3 的要求。

6.4.4 日志管理

查看并导出日志记录，结果应符合 5.4.4 的要求。日志格式应符合国家密码管理主管部门的要求。

6.4.5 管理员管理

用非法的身份或错误的口令登录，系统应拒绝；当连续重试次数到达系统设定的限制值时系统应锁定。

用合法的身份和正确口令登录，应能进入管理界面，进行相应的管理操作。

6.4.6 设备管理

6.4.6.1 设备初始化

对设备进行初始化操作，结果应符合 5.4.6.1 的要求。

6.4.6.2 设备注册

当系统有管理中心时，进行设备的注册等管理操作。结果应符合 5.4.6.2 的要求。

6.4.6.3 设备自检

对设备进行自检操作，结果应符合 5.4.6.3 的要求。

6.4.7 远程管理

检测结果应符合 5.4.7 的要求。

6.5 硬件检测

检测结果应符合 5.5 的要求，其中参考标准不作为强制要求。

6.6 参数可配置能力检测

检测结果应符合 5.6 的要求。

6.7 过程保护检测

检测结果应符合 5.7 的要求。

7 合格判定

本标准中，6.1、6.3、6.5 以及 6.4 中除 6.4.1、6.4.2、6.4.3、6.4.6.2、6.4.7 以外的各项要求中，其任意一项要求不合格，判定为产品不合格。