ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0023—2023
代替 GM/T 0023—2014

IPSec VPN 网关产品规范

IPSec VPN gateway product specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　发布

目　　次

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。

本文件代替 GM/T 0023—2014《IPSec VPN 网关产品规范》。与 GM/T 0023—2014 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了 GCM 可鉴别加密机制作为对称算法的工作机制（见 5.4 和 7.3）；

b) 增加了“热备份”“负载均衡”“对端探测”“网络适应性”“集群部署”“动态地址”的要求（见 5.11、5.12、5.13、5.14、5.15 和 5.16）；

c) 删除了“参数可配置能力要求”“过程保护”（见 2014 年版的 5.6 和 5.7）；

d) 增加了“密码协议要求”“算法配用要求”“密码部件调用接口要求”“敏感参数管理要求”的要求（见 7.2、7.3、7.4 和 7.5）；

e) 将“管理功能要求”更改为“管理要求”，并对内容进行了更改：删除了“合规性验证”，将“参数配置管理”更改为“配置管理”并增加了“配置数据管理”，将“远程监控管理”更改为“设备监控”并删除了“参数查询”，将“日志管理”更改为“日志功能”并合并到“设备监控”，删除了“远程管理”，增加了“管理协议和接口”，增加了远程配置管理、远程设备监控的协议和接口要求（见第 8 章，2014 年版的第 5 章）；

f) 将“检测要求”更改为“检测方法”，并按照新的章节结构和内容进行了相应更改（见第 10 章，2014 年版的第 6 章）；

g) 将“合格判定”更改为“判定规则”，并按照新的章节结构和内容进行了相应更改（见第 11 章，2014 年版的第 7 章）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中电科网络安全科技股份有限公司、四川大学、深信服科技股份有限公司、阿里云计算有限公司、鼎铉商用密码测评技术有限公司、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、山东得安信息技术有限公司、华为技术有限公司、天融信科技集团股份有限公司、西安交大捷普网络科技有限公司、山东大学。

本文件主要起草人：罗俊、龚勋、叶润国、张大江、邹家须、郑强、谭武征、李元正、徐明翼、徐强、王妮娜、马洪富、黄敏、孔凡玉。

本文件及其所代替文件的历次版本发布情况为：

——2014 年首次发布为 GM/T 0023—2014；

——本次为第一次修订。

IPSec VPN网关产品规范

1 范围

本文件规定了IPSec VPN网关产品的功能要求、性能要求、安全性要求、管理要求、硬件要求、检测方法和合格判定条件。

本文件适用于IPSec VPN网关产品的研制、使用和检测。

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 9813.3 计算机通用规范 第3部分：服务器

GB/T 15153.1 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 15843.1 信息技术 安全技术 实体鉴别 第1部分：总则

GB/T 15843.2 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 15843.4 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

GB/T 15843.5 信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GM/T 0005 随机性检测规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0022—2023 IPSec VPN技术规范

GM/T 0028 密码模块安全要求

GM/T 0062 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

AH：鉴别头(Authentication Header)

CBC：密文分组链接(Cipher Block Chaining)

DPD：对端探测(Dead Peer Detection)

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

GCM：Galois计数器模式(Galois Counter Mode)

IPSec:IP 安全(Internet Protocol Security)
IV:初始化向量(Initial Vector)
NAT:网络地址转换(Network Address Translation)
VPN:虚拟私有网络(Virtual Private Network)

5 功能要求

5.1 随机数生成

IPSec VPN 网关应具备独立的随机数生成功能。

5.2 工作模式

IPSec VPN 网关工作模式应支持隧道模式。

5.3 密钥交换

IPSec VPN 网关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—2023 中 6.1 的要求进行;
——密钥交换产生的工作密钥和会话密钥在 IPSec VPN 网关每次启动时均应置零。

5.4 安全报文封装

安全报文封装协议应支持 ESP 协议,宜支持 AH 协议与 ESP 协议嵌套使用:
——AH 协议与 ESP 协议嵌套使用时,不启用 ESP 协议中的验证操作;
——ESP 协议单独使用时,应启用 ESP 协议中的验证操作,当采用 GCM 可鉴别加密机制时,应采用 GCM 算法生成的 16 字节用于数据完整性校验的标签赋值 ESP 报文中的鉴别数据字段;
——安全报文封装协议应按照 GM/T 0022—2023 中 6.2 的要求进行。

5.5 NAT 穿越

IPSec VPN 网关单独使用 ESP 协议时应支持 NAT 穿越,NAT 穿越协议应符合 GM/T 0022—2023 中 6.1.4 的要求。

5.6 鉴别方式

IPSec VPN 网关应具有身份鉴别的功能,鉴别过程应按照 GM/T 0022—2023 中 6.1 的要求实现通信双方的身份鉴别。

5.7 IP 协议版本支持

IPSec VPN 网关应支持 IPv4 协议,宜支持 IPv6 协议。

5.8 抗重放攻击

IPSec VPN 网关在安全报文传输阶段应具有对抗重放攻击的功能。

5.9 密钥更新

IPSec VPN 网关应具有根据时间周期条件进行工作密钥和会话密钥更新的功能,宜具有根据报文

流量条件进行工作密钥和会话密钥更新的功能：

——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 $2^{10}\times2^{32}$ 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 $2^{10}\times2^{32}$ 字节。

5.10 包过滤

IPSec VPN 网关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，处理方式应支持丢弃、明文转发、密文转发（使用 IPSec 处理后转发）。

5.11 热备份

IPSec VPN 网关宜具有双机热备功能，具体实现方式为主-主或主-从模式，主从设备切换时，通信中断时间不大于 1 min。

5.12 负载均衡

IPSec VPN 网关宜支持多链路负载均衡，能为同一个五元组配置多个安全隧道，能对匹配该五元组的数据流采用轮询/加权轮询、随机/加权随机、哈希散列、最小负荷或其他方式并结合隧道状态进行安全隧道的选择。

5.13 对端探测

IPSec VPN 网关宜具有对端检测（DPD）功能，当检测到隧道对端在规定时间内没有响应的时候，删除该隧道，并在需要时重新发起密钥交换。

5.14 网络适应性

IPSec VPN 网关宜具有在 VLAN、VxLAN 网络环境中部署的能力，并支持 GRE over IPSec 和 L2TP over IPSec 封装模式。

5.15 集群部署

IPSec VPN 网关宜具有集群部署的能力，并支持集群内部 IPSec VPN 网关之间的安全策略、安全联盟和密钥的同步。

5.16 动态地址

IPSec VPN 网关宜具有支持网关 IP 地址动态变化的能力，能通过域名方式查询网关 IP 地址。

6 性能要求

6.1 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，配置 IPSec VPN 网关安全策略为密文转发，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。

6.2 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，配置 IPSec

VPN 网关安全策略为密文转发，在丢包率为 0 的条件下，数据报文通过 IPSec VPN 网关传输所消耗的平均时间。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。

6.3 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，配置 IPSec VPN 网关安全策略为密文转发，在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。

6.4 每秒新建隧道数

每秒新建隧道数是指 IPSec VPN 网关在 1 s 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。

6.5 最大并发隧道数

最大并发隧道数是指 IPSec VPN 网关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。

7 安全性要求

7.1 密钥管理要求

IPSec VPN 网关使用的密钥应具有唯一性，应来自于符合 GM/T 0005 随机性检测要求的尚未使用的有效随机数。密钥种类应符合 GM/T 0022—2023 的规定，包括以下类型。

a) 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：
   - 签名密钥对用于 IPSec VPN 网关及客户端的实体鉴别，由产品自身产生，其公钥应能被导出；
   - 加密密钥对用于工作密钥交换过程的保护，其保护结构应符合 GM/T 0016；
   - 设备密钥应保存在非易失性存储装置中，其私钥应有安全保护措施，在任何情况下不能以明文形式出现在产品外部；
   - 设备密钥应按设定的安全策略进行更新并应以安全形式进行备份，在需要时应能够恢复。
b) 工作密钥。对称算法使用的密钥，用于会话密钥交换过程的保护：
   - 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；
   - 达到工作密钥更新条件后应立即更换工作密钥；
   - 在连接断开、设备断电时应销毁工作密钥。
c) 会话密钥。对称算法使用的密钥，用于数据报文的机密性和完整性保护：
   - 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；
   - 达到会话密钥更新条件后应立即更换会话密钥；
   - 在连接断开、设备断电时应销毁会话密钥。

7.2 密码协议要求

IPSec VPN 网关应按照 GM/T 0022—2023 的规定，使用密钥交换协议进行安全联盟的协商、建立、修改、删除，单独使用封装安全载荷 ESP 协议或嵌套使用鉴别头 AH 协议和封装安全载荷 ESP 协议的方式为数据报文提供机密性、数据源鉴别、无连接完整性、抗重放攻击和有限信息流量的保护，具体协议报文格式应符合 GM/T 0022—2023。

7.3 算法配用要求

IPSec VPN 网关及客户端使用的密码算法应符合 GM/T 0022—2023 的规定，包括以下算法：

a) 非对称密码算法，应使用 SM2 椭圆曲线密码算法，用于网关及客户端的实体鉴别和工作密钥交换过程的保护；

b) 对称密码算法，应使用 SM4 分组密码算法，用于密钥交换数据和报文数据的机密性保护，用于密钥交换数据保护时，算法的工作模式应支持 CBC 模式，用于报文数据保护时，算法的工作模式应支持 CBC 或 GCM 模式，加密过程使用的初始化向量应具备一定的随机性；

c) 密码杂凑算法，应使用 SM3 算法，用于密钥交换数据和报文数据的完整性校验。

7.4 密码部件调用接口要求

IPSec VPN 网关应使用具有明确定义的函数接口调用密码部件进行对称、非对称、密码杂凑、随机数生成的密码运算。

7.5 敏感参数管理要求

IPSec VPN 网关的包括密钥在内的敏感安全参数的生成、建立、输入、输出、存储和置零的全生命周期的管理应符合 GM/T 0028 的要求。

7.6 硬件安全要求

IPSec VPN 网关的硬件符合以下安全要求。

——应符合 GM/T 0028 对硬件模块物理安全的规定。

——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，不应提供任何可供调试、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认证作为安全措施。

——应防止通过非授权的任何外部接口获得设备中的敏感信息。

——在工艺设计、结构设计、硬件配置方面应采取相应的保护措施，保证设备基本的物理安全防护功能。

7.7 软件安全要求

IPSec VPN 网关的软件和固件符合以下安全要求：

——应符合 GM/T 0028 对软件/固件安全的规定；

——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，裁减一切不需要的功能，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，应不能泄露密钥和敏感信息；

——应只接受合法的操作指令。

8 管理要求

8.1 配置管理

8.1.1 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)、源端口和目的端口(针对 TCP 和 UDP)或 ICMP 请求类型构成一个五元组,五元组加上对匹配该五元组的数据报文的处理方式:丢弃、明文转发或密文转发(使用 IPSec 处理后转发)构成一条 IPSec 安全策略,其中密文转发安全策略应包括对应的 IPSec 安全联盟。IPSec VPN 网关应提供对其 IPSec 安全策略进行添加、删除、修改、查询操作的接口。

8.1.2 安全参数配置

IPSec VPN 网关应提供对其安全参数进行添加、删除、修改、查询操作的接口,安全参数宜包括安全联盟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。

8.1.3 网络参数配置

IPSec VPN 网关应提供对其网络参数进行添加、删除、修改、查询操作的接口,网络参数宜包括网络接口的 IP 地址和 MAC 地址、网络接口的 MTU(最大传输单元)、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、TCP MSS(最大分段大小)。

8.1.4 用户参数配置

当支持客户端模式时,IPSec VPN 网关应提供对其用户参数进行添加、删除、修改、查询操作的接口,用户参数宜包括用户名和口令、用户配置信息(包括接入用 IP 地址、网关 IP 地址、DNS 服务器地址)、用户有效期。

8.1.5 其他参数配置

IPSec VPN 网关宜提供对其他功能模块的参数进行添加、删除、修改、查询操作的接口。

8.1.6 配置数据管理

IPSec VPN 网关应保证重要配置数据在设备中的完整性、可靠性,应提供重要配置数据的备份恢复功能。

8.2 设备监控

8.2.1 状态监测

IPSec VPN 网关宜提供对其运行状态(包括 CPU、内存和易失性存储介质的占有率)、系统信息(包括开机时间、运行时间、系统时间和设备名字及 IP)、网络流量、是否在线、密码部件工作是否正常、隧道状态(包括建立时间、加密流量、有效期)进行实时查询的接口,并在设备状态异常时发出告警。

8.2.2 远程控制

IPSec VPN 网关宜提供对其进行重启、故障诊断、各项功能的关闭和启用操作的接口。

8.2.3 时间同步

IPSec VPN 网关宜提供对其进行时间同步的接口。

8.2.4 日志功能

IPSec VPN 网关应提供日志功能,日志应能被查看、导出。日志的记录要素应包括事件发生的日期、时间、主体、客体、类型和结果。日志内容应包括:

a） 操作行为，登录认证、参数配置、策略配置、密钥管理操作；
b） 安全事件，密钥交换成功及失败、密钥过期、隧道建立及删除事件；
c） 异常事件，解密失败、完整性校验失败事件的统计。

8.3 设备管理

8.3.1 设备初始化

IPSec VPN 网关的初始化，除应由生产厂商进行的操作外，设备密钥的生成和管理员的产生操作均应由使用者完成。初始化数据中如含有私钥，应提供安全硬件介质承载，安全硬件介质应通过商用密码检测认证。

8.3.2 设备注册

IPSec VPN 网关宜具有向管理中心进行自动注册的功能。

8.3.3 设备自检

IPSec VPN 网关每次启动时均进行自检：

——应对密码运算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；
——应对存储的包括密钥在内的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；
——应按照 GM/T 0062 对 E 类产品的规定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，随机数产生质量应符合 GM/T 0005 的要求；
——应对表征身份的介质及其接口进行检查，确保其正常工作；
——宜对 CPU、内存、网络接口、非易失性存储介质以及其他主要物理部件进行常规检查，确保各关键部件正常工作；
——在检查不通过时应发出告警并停止工作。

8.4 管理员要求

IPSec VPN 网关设置管理员：

——管理员进行设备的配置管理以及设备密钥的生成、导入、备份和恢复操作，管理员应持有表征身份信息的硬件介质，与登录口令相结合登录系统，管理员进行管理操作前应通过实体鉴别并应符合 GB/T 15843.1～GB/T 15843.5 的要求；
——宜实现系统管理员、安全管理员、审计管理员分权管理，安全管理员负责设备的配置管理和设备密钥的生成、导入、备份和恢复操作，系统管理员负责设备日常运行的管理和维护，对管理员角色进行添加、删除、修改、查询操作和管理权限分配，以及对设备重要数据的备份和恢复，审计管理员负责对设备的日志进行安全审计；
——管理员只能通过被授权的终端登录到 IPSec VPN 网关进行相应的操作，授权方式宜包括对终端的 IP 进行授权；
——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。

8.5 管理协议和接口

IPSec VPN 网关的远程配置管理和远程设备监控功能，应使用安全的协议和接口，建立安全通道，进行实体鉴别以及消息的机密性和完整性保护：

——如果采用传输层密码协议(TLCP)，应符合 GB/T 38636 的规定；

——如果采用 IPSec 协议，应符合 GM/T 0022—2023 的规定；

——如果采用自定义密码协议，应符合密码国家标准、行业标准的相关要求。

9 硬件要求

9.1 外部接口

IPSec VPN 网关具备外部接口：

——应至少具备两个工作网口；

——应支持双臂(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；

——宜支持单臂接入(以单个网络接口用旁路的方式将设备接入网络)；

——应具备管理接口，管理接口宜通过 TCP/IP 网络或串行接口与管理设备连接。

9.2 密码部件

IPSec VPN 网关应采用通过商用密码检测认证的密码模块或安全芯片作为密码部件实现密码运算和密钥管理。

9.3 随机数发生器

IPSec VPN 网关采用的随机数发生器应通过商用密码检测认证，生成的随机数应由多路硬件随机源产生并符合 GM/T 0005 的要求，至少采用两个独立的物理噪声源芯片实现。

9.4 环境适应性

IPSec VPN 网关应遵守 GB/T 9813.3 中关于气候环境适应性的相关要求。

9.5 电磁兼容性

IPSec VPN 网关应遵守 GB/T 15153.1 中关于电磁兼容等级的相关要求。

9.6 可靠性

IPSec VPN 网关的平均无故障工作时间应不低于 10 000 h，平均可持续加密流量应不低于 10 000 Gb，宜使用双机热备、集群或负载均衡部署方式提高可靠性。

10 检测方法

10.1 检测说明

检测要求规定了 IPSec VPN 网关的通用检测内容和方法。检测应包括外观和结构检查、提交文档的检查、功能检测、性能检测、安全性检测、管理检测和硬件检测。

10.2 外观和结构的检查

根据产品的物理参数，对被检测设备的外观、尺寸、内部部件及附件进行检查。

10.3 提交文档的检查

被检测设备研制单位应按照具备资格的商用密码检测、认证机构的检测要求提交相关文档资料，作为 IPSec VPN 网关的检测认证依据。

10.4 功能检测

10.4.1 随机数功能

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 GM/T 0005 的要求。

10.4.2 工作模式

将检测设备与被检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。

10.4.3 密钥交换

进行密钥交换功能检测时：

——按 GM/T 0022—2023 中 6.1.3 的方法进行密钥交换，将检测设备与被检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—2023 中 6.1.3 的要求，其报文格式应符合 GM/T 0022—2023 中 6.1.5 的要求。

10.4.4 安全报文封装协议

进行安全报文封装功能检测时：

——将检测设备与被检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—2023 中 6.2.2 的要求；

——当 IPSec VPN 网关支持 AH 协议与 ESP 协议嵌套使用时，将检测设备与被检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—2023 中 6.2.1 和 6.2.2 的要求。

10.4.5 NAT穿越

进行 NAT 穿越功能检测时：

——将被检测设备放在 NAT 环境下，按 GM/T 0022—2023 中 6.1.3 的方法进行密钥交换，将检测设备与被检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—2023 中 6.1.3 的要求，其报文格式应符合 GM/T 0022—2023 中 6.1.5 的要求；

——将检测设备与被检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—2023 中 6.2.2 和 6.2.3 的要求。

10.4.6 鉴别方式

按 GM/T 0022—2023 中 6.1.3 的方法进行密钥交换，通信双方应能实现双向身份鉴别，成功完成交换过程，建立 IPSec 隧道进行通信。

10.4.7 IP协议版本支持

在 IPv4 或者 IPv6 的环境下，按 GM/T 0022—2023 中 6.1.3 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。

10.4.8 抗重放攻击

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

10.4.9 密钥更新

进行密钥更新功能检测时：

——在检测设备和被检测设备上按照相同参数分别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，在检测设备和被检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。

10.4.10 包过滤

在被检测设备上分别配置不同五元组对应 IPSec 策略的处理选择为丢弃、明文转发或密文转发(使用 IPSec 处理)，利用检测设备在被检测设备的内网口发送前述不同五元组的数据报文，在被检测设备的外网口应不能检测到设定为丢弃的数据报文、应检测到设定为明文转发的数据报文明文、应检测到设定为密文转发的数据报文密文。

10.5 性能检测

10.5.1 加解密吞吐率

根据 6.1 的加解密吞吐率定义，将被检测设备连接检测设备进行检测，检测结果的数据应无明显异常。

10.5.2 加解密时延

根据 6.2 的加解密时延定义，将被检测设备连接检测设备进行检测，检测结果的数据应无明显异常。

10.5.3 加解密丢包率

根据 6.3 的加解密丢包率定义，将被检测设备连接检测设备进行检测，检测结果的数据应无明显异常。

10.5.4 每秒新建隧道数

根据 6.4 的每秒新建隧道数定义，将被检测设备连接检测设备进行检测，检测结果的数据应无明显异常。

10.5.5 最大并发隧道数

根据 6.5 的最大并发隧道数定义，将被检测设备连接检测设备进行检测，检测结果的数据应无明显异常。

10.6 安全性检测

10.6.1 密钥管理

对被检测设备进行设备密钥的产生或导入、备份、恢复以及更新操作，并对被检测设备工作过程中工作密钥和会话密钥的产生、使用、存储、更新和销毁进行检查，检查结果应符合 7.1 的要求。

10.6.2 密码协议

按照 10.4.3、10.4.4 和 10.4.5 进行检测。

10.6.3 算法配用

检查被检测设备，能够按照 7.3 的要求设置密码算法。

10.6.4 密码部件调用接口

对被检测设备研制单位提供的密码部件调用接口相关源代码或说明文档进行检查，检查结果应符合 7.4 的要求。

10.6.5 敏感参数管理

对被检测设备的包括密钥在内的敏感安全参数进行生成、建立、输入、输出、存储和置零操作，操作结果应符合 7.5 的要求。

10.6.6 硬件安全

对被检测设备的硬件进行检查，并检查被检测设备研制单位提供的设计文档和产品安全性承诺，检查结果应符合 7.6 的要求。

10.6.7 软件安全

使用漏洞扫描工具检查被检测设备的端口和服务，并检查被检测设备研制单位提供的设计文档、源代码和产品安全性承诺，检查结果应符合 7.7 的要求。

10.7 管理检测

10.7.1 配置管理

对被检测设备进行安全策略、安全参数、网络参数、用户参数的添加、删除、修改、查询操作，并对重要配置数据进行完整性检查和备份恢复操作，检查结果应符合 8.1 的要求，可配置项的数量应不少于设备正常工作所必需的配置项。

10.7.2 设备监控

进行设备监控功能检测时：

——对被检测设备的运行状态进行检查，并进行异常操作（例如，中断网络连接或停止密码部件工作），被检测设备应发出告警；

——对被检测设备的日志内容进行检查，检查结果应符合 8.2.4 的要求。

10.7.3 设备管理

进行设备管理功能检测时：

——对被检测设备进行初始化操作，操作过程及结果应符合 8.3.1 的要求；

——通过拔插或关停关键部件并查看设备状态以及查看日志的方式检查被检测设备自检功能，检查结果应符合 8.3.3 的要求。

10.7.4 管理员

对被检测设备进行管理员登录操作，操作过程及结果应符合 8.4 的要求。

10.7.5 管理协议和接口

如果被检测设备具备远程配置管理或远程设备监控功能，对被检测设备进行远程配置管理、远程设备监控操作，并对通信的报文进行网络数据截获，检查采用的协议及接口，检查结果应符合 8.5 的要求。

10.8 硬件检测

10.8.1 外部接口

对被检测设备的外部接口进行检查，检查结果应符合 9.1 的要求。

10.8.2 密码部件

对被检测设备的密码部件进行检查，检查结果应符合 9.2 的要求。

10.8.3 随机数发生器

对被检测设备的随机数发生器进行检查，检查结果应符合 9.3 的要求。

10.8.4 其他硬件

对被检测设备的环境适应性、电磁兼容性和可靠性进行检查，检查结果应分别符合 9.4～9.6 的相关要求。

11 判定规则

第 10 章的各项检测中，除 10.5 和 10.8.4 以外的任意一项检测结果不合格，则判定为产品密码检测不合格。