ICS 33.050
CCS M30

团　体　标　准

T/TAF 330—2026

网络设备密码应用测试方法　防火墙设备

Cryptography application test method for network devices—
Firewall devices

2026-02-09 发布　　2026-02-09 实施

电信终端产业协会　发布

版权声明

邮箱：tafrb@taf.org.cn

电话：010-8205280

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。

请注意本文件中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。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、郑州信大捷安信息技术股份有限公司、上海泰峰检测认证有限公司、武汉网锐检测科技有限公司、成都泰瑞通信设备检测有限公司、华为技术有限公司、中兴通讯股份有限公司、北京通和实益电信科学技术研究所有限公司、新华三技术有限公司、博鼎实华（北京）技术有限公司、深圳信息通信研究院。

本文件主要起草人：刘欣东、张治兵、张亚薇、彭金辉、刘为华、宋祥烈、罗志达、陈玺、龚志红、吴翔宇、陈鹏、陈泽、周继华、张大超、韩娟、万晓兰、付志强、刘向东、王玥、唐伟生。

网络设备密码应用测试方法　防火墙设备

1　范围

本文件规定了网络型防火墙设备在软件/固件安全、身份鉴别、访问控制、网络通信安全、数据安全、计算安全的密码应用测试方法与密码应用的性能测试方法。

本文件适用于在我国境内销售或提供的网络型防火墙设备，也可为网络运营者采购网络型防火墙设备时提供依据，还适用于指导网络型防火墙设备的研发、测试等工作。

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 25069—2022　信息安全技术　术语

GB/T 32915—2016　信息安全技术　二元序列随机性检测方法

GM/T 0005—2021　随机性检测规范

T/TAF 217—2024　网络设备密码应用技术要求　防火墙设备

3　术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

防火墙　firewall

对经过的数据流进行解析，并实现访问控制及安全防护功能的网络安全产品。

注：根据安全目的、实现原理的不同，通常可分为网络型防火墙、WEB应用防火墙、数据库防火墙和主机型防火墙等。

[来源：GB/T 20281—2020，3.1]

3.2

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.3

解密　decipherment/decryption

对密文进行密码变换以产生数据的过程。

3.4

密钥 key

控制密码算法运算的关键信息或参数。

3.5

保密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.6

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.7

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

3.8

重要数据 important data

主要指防火墙设备的重要数据，包括身份鉴别信息、访问控制信息、配置信息、日志信息、升级数据、远程配置指令、告警信息、密钥等，具体参见附录A。

3.9

可信计算环境 trusted execution environment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

3.10

固件 firmware

固件（Firmware）是写入EPROM（可擦写可编程只读存储器）或EEPROM（电可擦可编程只读存储器）中的程序。

4 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

DES：数据加密标准（Data Encryption Standard）

MAC：消息鉴别码（Message Authentication Code）

MD5：信息摘要算法（Message-Digest Algorithm）

SHA：安全散列算法（Secure Hash Algorithm）

UDP：用户数据报协议（User Datagram Protocol）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IPSec：互联网安全协议（Internet Protocol Security）

SSH：安全外壳协议（Secure Shell）

SSL：安全套接层（Secure Socket Layer）

SNMP：简单网络管理协议（Simple Network Management Protocol）
VPN：虚拟专用网络（Virtual Private Network）

5 测试环境

测试环境如图1、图2、图3、图4所示。

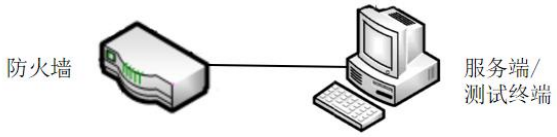

图1 测试环境1

测试环境1描述：被测设备与服务端/测试终端相连。

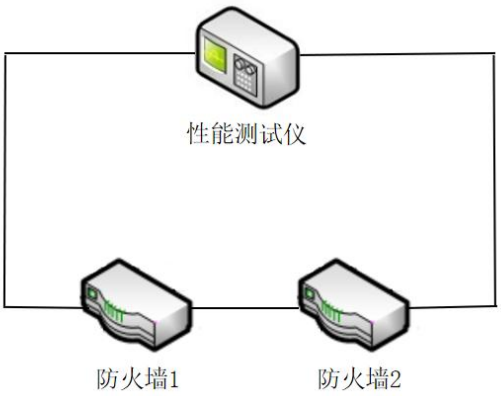

图2 测试环境2

测试环境2描述：性能测试仪用于模拟真实业务流量。

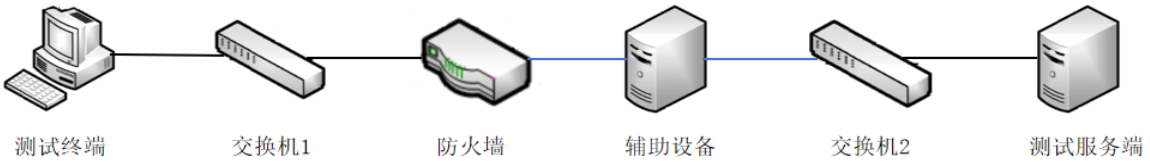

图3 测试环境3

测试环境3描述：测试使用IPSec等需要两端建立隧道的方法时使用辅助设备（用于与被测设备建立IPsec隧道），如不使用IPSec相关方式则无需使用辅助设备，测试终端访问测试服务端形成测试业务流量。

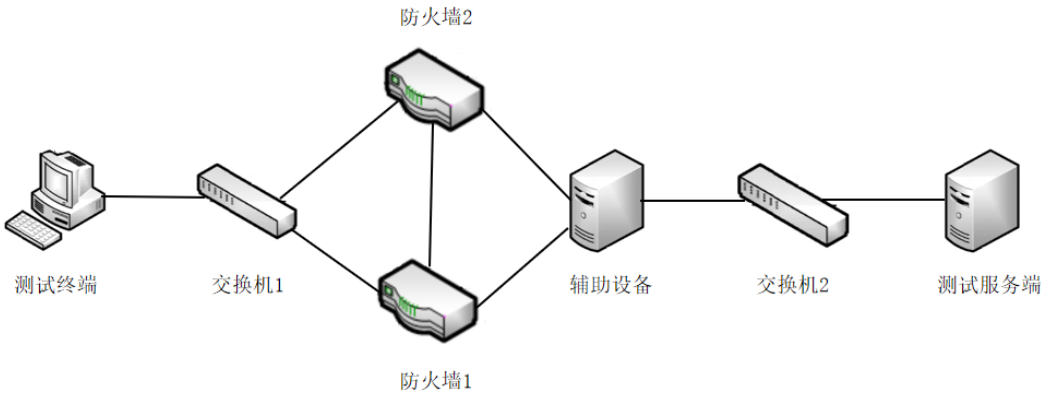

图4　测试环境4

测试环境4描述：测试使用IPSec等需要两端建立隧道的方法时使用辅助设备（用于与被测设备建立IPsec隧道），如不使用IPSec相关方式则无需使用辅助设备，测试PC访问测试服务端形成测试业务流量。

6　防火墙设备密码应用测试方法

6.1　密码基本应用要求测试

6.1.1　密码管理

密码管理测试方法如下：

a）　安全要求：

1）　应包含密钥产生、密钥存储、密钥使用、密钥更新等功能（T/TAF 217—2024 5.1a））；

2）　应按照密钥更新周期要求更新密钥（T/TAF 217—2024 5.1b））；

3）　应有安全措施防止密钥的泄露和替换（T/TAF 217—2024 5.1c））；

4）　首次使用公钥前，应对证书有效性进行验证（T/TAF 217—2024 5.1d））。

b）　预置条件：

1）　按测试环境 1 搭建好测试环境；

2）　厂商提供被测设备预装软件，并完成安装；

3）　厂商应提供被测设备密钥管理技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c）　检测方法：

1）　检查厂商提供的密钥管理技术说明，是否覆盖包括密钥产生（当被测设备支持时）、密钥存储、密钥使用、密钥更新、密钥销毁的密钥全生命周期过程；

2）　检查被测设备是否根据管理技术说明包含密钥产生（当被测设备支持时）、密钥存储、密钥使用、密钥更新、密钥销毁等功能；

3）　检查被测设备在达成密钥更新的条件时是否自动更新密钥，或提醒用户手动更新密钥；

4）　对于厂商说明中列出的用于防止密钥的泄露和替换的安全措施，检查被测设备是否正确实现了这些措施，例如若仅管理员可以查看/修改密钥，应确认其他权限的用户无法执行相关命令等；

5） 在首次使用公钥前，使用有效证书，检查是否可以通过被测设备的验证；修改/替换该证书，使其变为无效证书，再次检查是否可以通过被测设备的验证；

6） 确认被测设备中涉及校验证书有效期和证书有效性的业务场景，使用有效证书，检查是否可以通过被测设备的验证；使用过期的证书，检查是否可以通过被测设备的验证；吊销有效证书，检查是否可以通过被测设备的验证；

7） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，厂商提供的密钥管理技术说明覆盖包括密钥产生（当被测设备支持时）、密钥存储、密钥使用、密钥更新、密钥销毁的密钥全生命周期过程，并符合国家相关规定的要求；

2） 检测方法步骤 2）中，被测设备包含密钥产生（当被测设备支持时）、密钥存储、密钥使用、密钥更新、密钥销毁等功能；

3） 检测方法步骤 3）中，在达成密钥更新的条件时被测设备触发自动更新密钥，或提醒用户手动更新密钥；

4） 检测方法步骤 4）中，被测设备实现了厂商说明中列出的用于防止密钥的泄露和替换的安全措施；

5） 检测方法步骤 5）中，有效证书可以通过被测设备的验证，修改/替换该证书后无法通过被测设备的验证；

6） 检测方法步骤 6）中，对于被测设备中涉及校验证书有效期及证书有效性的业务场景，有效期内的证书可以通过被测设备的验证，过期的证书无法通过被测设备验证，被吊销的证书无法通过被测设备的验证；

7） 检测方法步骤 7）中，检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.1.2 密码随机性

密码随机性测试方法如下：

a） 安全要求：

应使用符合 GB/T 32915-2016 标准的随机数生成器，显著性水平参考 GM/T 0005—2021（T/TAF 217—2024 5.1e））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备中随机数生成器的输入输出接口或指令；

4） 厂商应提供被测设备生成随机数所采用密码技术的说明，说明内容应包含使用的密码技术名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 使用 GB/T 32915—2016 标准的检测方法或提供证明材料验证被测设备生成的随机数是否达到了 GM/T 0005—2021 的测试指标要求；

2） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，随机数生成器应能够通过 GB/T 32915—2016 标准的检测，达到 GM/T 0005-2021 的测试指标要求，或提供的证明材料证明密码随机性达到 GM/T 0005—2021 的测试指标要求；

2） 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.1.3 密码算法强度

密码算法强度测试方法如下：

a） 安全要求：

设备使用的密码技术（指本文件规定范围内的密码应用技术）应支持使用安全强度较高的密码算法，不宜使用安全强度弱的密码算法（T/TAF 217—2024 5.1f））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备密码算法的调用接口或指令；

4） 厂商应提供被测设备采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查以上使用的密码技术是否使用强密码算法，即当前在业界普遍认可，且具有可证明安全性或在当前的算力环境下显著不可破解的密码算法；

2） 检测被测设备是否正确使用了厂商声明的密码算法；

3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，上述使用的密码技术使用了强密码算法，没有发现使用安全强度弱的密码算法，或可关闭使用安全强度弱的密码算法，如 md5、SHA1、DES 等；

2） 检测方法步骤 2）中，被测设备正确使用了厂商声明的密码算法；

3） 记录的密码技术信息应与厂商提供的材料一致。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.2 软件/固件密码应用测试

6.2.1 软件/固件升级

软件/固件升级测试方法如下：

a） 安全要求：

升级时，应使用密码技术保证固件/软件升级包的完整性与身份校验(T/TAF 217—2024 5.2a))。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商提供被测设备预装软件/固件的更新包；

3） 厂商提供签名验证的工具或指令；

4） 厂商应提供被测设备保证软件/固件升级采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查厂商发布更新软件包时是否同时发布更新软件包和数字签名；

2） 使用工具或指令验证厂商提供的更新包，检查是否通过签名验证；

3） 修改厂商提供的预装软件更新包、使用工具或指令验证修改过的更新包、检查是否可以通过完整性校验；

4） 修改预装软件升级包的数字签名，检查是否能通过签名验证；

5） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 更新包与签名一同发布；

2） 使用厂商提供的预装软件更新包进行签名验证，若更新包与签名不匹配，则验证不通过，输出错误信息；若匹配，则输出验证通过信息；

3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.2.2 软件/固件保密性

软件/固件保密性测试方法如下：

a） 安全要求：

可使用密码技术保证软件/固件保密性（T/TAF 217—2024 5.2b））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备保证软件/固件保密性采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查是否可采用密码技术的加解密功能对软件/固件进行保护，并验证保护机制是否有效；

2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，可以采用加解密功能进行保护，保护机制有效；

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.2.3 软件/固件完整性

软件/固件完整性测试方法如下：

a） 安全要求：

可使用密码技术保证软件/固件完整性（T/TAF 217—2024 5.2c））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备保证软件/固件完整性采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查是否可采用密码技术对固件/软件的完整性进行保护，并验证保护机制是否有效；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，可以采用密码技术进行固件/软件的完整性保护，保护机制有效；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.2.4 软件/固件抵御攻击能力

软件/固件抵御攻击能力测试方法如下：

a） 安全要求：
可使用密码技术保证软件/固件抵御常见的攻击，如反编译、重打包等（T/TAF 217—2024 5.2d））。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备保证软件/固件加固（如反编译、重打包等）采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查是否采用有效的密码技术抵御反编译、重打包等攻击；
2） 若被测设备使用了开源的密码算法实现，检查该开源实现是否存在可利用的公开漏洞；
3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，有效采用了密码技术抵御反编译、重打包等攻击；
2） 检测方法步骤 2）中，被测设备中使用的开源密码算法实现不存在可利用的公开漏洞；
3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.2.5 软件/固件启动

软件/固件启动测试方法如下：

a） 安全要求：
启动时，可使用密码技术证明设备内软件/固件的完整性与身份校验(T/TAF 217—2024 5.2e))。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件/固件；
3） 厂商提供签名验证的工具或指令；
4） 厂商应提供被测设备保证软件/固件启动采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查厂商提供预装软件/固件时是否可以同时提供预装软件/固件和数字签名；
2） 使用工具或指令验证厂商提供的预装软件/固件，检查是否可以通过签名验证；

3） 修改厂商提供的预装软件包、使用工具或指令验证修改过的预装软件包/固件，检查是否可以通过完整性校验；
4） 修改预装软件包/固件的数字签名，检查是否可以通过签名验证；
5） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 预装软件包/固件与签名可以一同发布；
2） 可以使用厂商提供的预装软件包/固件进行签名验证，若预装软件包/固件与签名不匹配，则验证不通过并可以输出错误信息，若匹配，则可以输出验证通过信息；
3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.3 身份鉴别密码应用测试

6.3.1 身份鉴别功能

身份鉴别功能测试方法如下：

a） 安全要求：
应使用密码技术对访问防火墙设备的实体（终端、软件或用户）进行身份鉴别，可使用密码技术进行双向身份鉴别（T/TAF 217—2024 5.3a））。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备身份鉴别功能采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对访问控制实体进行身份鉴别/双向身份鉴别；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，采用了密码技术进行身份鉴别/双向身份鉴别；
2） 记录的密码算法信息与厂商提供的材料一致，密码算法安全强度符合标准要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.3.2 身份鉴别信息保密性

身份鉴别信息保密性测试方法如下：

a） 安全要求：
1） 应使用密码技术保证身份鉴别信息传输过程中的保密性（T/TAF 217—2024 5.3b））；
2） 应使用密码技术保证身份鉴别信息存储过程中的保密性（T/TAF 217—2024 5.3c））。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备身份鉴别信息安全保护中采用密码技术的说明，说明内容应包含使用

的密码算法名称、用途、何处使用及其实现方式。

c) 检测方法：

1) 按照厂商提供说明材料，传输用户身份鉴别信息，通过抓包或其他有效的方式查看是否以加密方式传输；

2) 按照厂商提供说明材料，生成用户身份鉴别信息，查看是否以加密方式存储；

3) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 1）中，厂商使用了加密方式传输，保护机制有效；记录的密码算法信息与厂商提供的材料一致，密码算法安全强度符合标准要求；

2) 检测方法步骤 2）中，身份鉴别信息以加密方式存储，保护机制有效；记录的密码算法信息与厂商提供的材料一致，密码算法安全强度符合标准要求。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3.3 身份鉴别信息完整性

身份鉴别信息完整性测试方法如下：

a) 安全要求：

1) 可使用密码技术保证身份鉴别信息传输过程中的完整性（T/TAF 217—2024 5.3d））；

2) 可使用密码技术保证身份鉴别信息存储过程中的完整性（T/TAF 217—2024 5.3e））。

b) 预置条件：

1) 按测试环境 1 搭建好测试环境；

2) 厂商提供被测设备预装软件，并完成安装；

3) 厂商应提供被测设备身份鉴别信息安全保护中采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c) 检测方法：

1) 按照厂商提供说明材料，传输用户身份鉴别信息，通过中间人劫持修改数据包信息或其他有效的方式查看是否验证传输信息的完整性；

2) 按照厂商提供说明材料，生成用户身份鉴别信息并存储，将存储的信息部分修改，查看是否验证存储信息的完整性；

3) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 1）中，传输的身份鉴别信息无法通过完整性验证，保护机制有效；

2) 检测方法步骤 2）中，存储的身份鉴别信息无法通过完整性验证，保护机制有效。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3.4 抵御重放攻击

抵御重放攻击测试方法如下：

a) 安全要求：

可使用密码技术来抵御常见的重放攻击，如伪随机数等（T/TAF 217—2024 5.3f））。

b) 预置条件：

1) 按测试环境 1 搭建好测试环境；

2) 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备防重放功能采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 查看厂商提供的说明资料，检查是否论证了所采用密码技术抵御重放攻击的技术原理，验证特定场景抗重放的能力；

2） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中， 厂商提供的说明资料正确且充分论证了所采用密码技术抵御重放攻击的技术原理，并且在特定场景下能够通过抗重放攻击的验证（如伪随机数等）；

2） 记录的密码算法信息与厂商提供的材料一致，密码算法安全强度符合标准要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.4 访问控制密码应用测试

6.4.1 访问控制功能

访问控制功能测试方法如下：

a） 安全要求：

可使用密码技术保障访问控制功能安全性，如数字证书等（T/TAF 217—2024 5.4a））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商应提供被测设备在执行访问控制功能时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检测设备授权的管理员（如系统管理员）下发和存储系统的访问控制配置时是否采用了密码技术；

2） 查看被测设备的访问控制功能在实施时所采用的密码技术是否能保障访问控制功能的安全性。

3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）、2）中，被测设备在下发和存储访问控制配置时，使用了密码技术来保证访问控制功能的安全性；

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.4.2 访问控制信息保护

访问控制信息保护测试方法如下：

a） 安全要求：

可使用密码技术保证访问控制信息的完整性（T/TAF 217—2024 5.4b））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商应提供被测设备在执行访问控制功能时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检测设备在下发和存储访问控制配置时是否采用密码技术保证访问控制配置的完整性；

2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，被测设备在下发和存储访问控制配置时，使用密码技术来保证访问控制功能的完整性；

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.5 网络通信安全密码应用测试

6.5.1 网络通信可信信道/可信路径

网络通信可信信道/可信路径测试方法如下：

a） 安全要求：

远程管理时，应支持使用密码技术建立可信信道/可信路径：

1） 在支持 web 管理时，应支持 HTTPS，并避免使用安全强度弱的密码算法与加密模式；

2） 在支持 SSH 管理时，应支持 SSHv2，并避免使用安全强度弱的密码算法与加密模式；

3） 在支持 SNMP 管理时，应支持 SNMPv3，应使用 authPriv 模式；

4） 在支持 Netconf 管理时，安全传输层应避免使用安全强度弱的密码算法与加密模式（T/TAF 217—2024 5.5a））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商应提供被测设备网络通信时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检测被测设备在建立可信信道/可信路径时所使用的密码技术；

i. 在支持 web 管理时，检测被测设备支持的 web 管理协议，是否使用安全强度弱的密码算法与加密模式，是否可关闭使用的安全强度弱的密码算法与加密模式；

ii. 在支持 SSH 管理时，检测被测设备支持的 SSH 管理协议版本，是否使用安全强度弱的密码算法与加密模式，是否可关闭使用的安全强度弱的密码算法与加密模式；

iii. 在支持 SNMP 管理时，检测被测设备支持的 SNMP 管理协议版本，是否使用 authPriv 模式；

iv. 在支持 Netconf 管理时，检测被测设备在安全传输时是否使用或可关闭安全强度弱的密码算法与加密模式。

2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，被测设备支持使用密码技术建立可信信道/可信路径；

i. 在支持 web 管理时，应支持 HTTPS，并避免使用或可关闭安全强度弱的密码算法与加密模式；

ii. 在支持 SSH 管理时，应支持 SSHv2，并避免使用或可关闭安全强度弱的密码算法与加密模式；

iii. 在支持 SNMP 管理时，应支持 SNMPv3，使用 authPriv 模式；

iv. 在支持 Netconf 管理时，安全传输层避免使用或可关闭安全强度弱的密码算法与加密模式。

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.5.2 网络通信重要数据传输

网络通信重要数据传输测试方法如下：

a） 安全要求：

1） 在使用 IPsec VPN 或 SSL VPN 时，应避免使用安全强度弱的密码算法与加密模式（T/TAF 217—2024 5.5b））；

2） 应使用密码技术保证路由协议认证功能的安全（T/TAF 217—2024 5.5c））；

3） 可使用通信数据加密后再传输的方式保证信息不被泄露（T/TAF 217—2024 5.5d））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商应提供被测设备网络通信时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检测被测设备在使用 IPsec VPN 或 SSL VPN 时，是否使用或可关闭安全强度弱的密码算法与加密模式；

2） 检测被测设备在路由协议认证时是否使用密码技术保证该功能的安全；

3） 检测被测设备在网络通信传输重要数据时是否采取安全措施保证信息不被泄露，如数据加密后再传输等方式；

4） 检查并记录以上功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，在使用 IPsec VPN 或 SSL VPN 时，避免使用或可关闭安全强度弱的密码算法与加密模式；

2） 检测方法步骤 2）中，在路由协议认证时使用密码技术保证该功能的安全；

3） 检测方法步骤 3）中，在网络通信传输重要数据时可使用通信数据加密后再传输等方式保证信息不被泄露；

4） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6 数据安全密码应用测试

6.6.1 远程配置指令传输保密性和完整性

远程配置指令传输保密性和完整性测试方法如下：

a） 安全要求：

应使用密码技术保证远程配置指令在传输过程中的保密性与完整性，如接受集中管理平台管理或与其他安全设备联动时下发的安全策略等（T/TAF 217—2024 5.6a））。

b) 预置条件：

1) 按测试环境 1 搭建好测试环境；

2) 厂商提供在传输过程中为保护远程配置指令传输过程中的保密性和完整性所使用的密码算法说明文档材料；

3) 厂商提供被测设备所涉及的远程配置指令清单。

c) 检测方法：

1) 通过人工查看和工具验证，检查传输远程配置指令是否有保密性和完整性保护措施，是否通过密码算法保证远程配置指令在传输过程中的保密性和完整性；

2) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 1）中，被测设备支持使用密码技术保证远程配置指令传输过程中的保密性和完整性；

2) 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.2 告警信息传输完整性

告警信息传输完整性测试方法如下：

a) 安全要求：

应使用密码技术保证告警信息在传输过程中的完整性，如向集中管理平台上报的安全事件、故障告警等（T/TAF 217—2024 5.6b））。

b) 预置条件：

1) 按测试环境 1 搭建好测试环境；

2) 厂商提供在传输过程中为保护告警信息完整性所使用的密码算法说明文档材料；

3) 厂商提供被测设备所涉及的告警信息清单。

c) 检测方法：

1) 通过人工查看和工具验证，检查传输的告警信息是否有完整性保护措施，是否通过密码算法保证告警信息传输过程中的完整性；

2) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 1）中，被测设备支持使用密码技术保证告警信息传输过程中的完整性；

2) 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.3 重要数据传输保密性和完整性

重要数据传输的保密性和完整性测试方法如下：

a) 安全要求：

可使用密码技术保证配置信息、日志信息等重要数据在传输过程中的保密性和完整性（T/TAF 217—2024 5.6c））。

b) 预置条件：

1） 按测试环境 1 搭建好测试环境；
2） 厂商提供在传输过程中为保护重要数据保密性和完整性所使用的密码算法说明文档材料；
3） 厂商提供被测设备所涉及的重要数据清单。

c） 检测方法：
1） 通过人工查看和工具验证，检查传输的重要数据是否有保密性和完整性保护措施，是否可通过密码算法保证重要数据的保密性和完整性；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，被测设备可支持使用密码技术保证重要数据传输过程中的保密性和完整性；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.4 重要数据存储保密性和完整性

重要数据存储的保密性和完整性测试方法如下：

a） 安全要求：
可使用密码技术保证配置信息、日志信息等重要数据在存储过程中的保密性和完整性（T/TAF 217—2024 5.6d））。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供在存储过程中为保护重要数据保密性和完整性所使用的密码算法说明文档材料；
3） 厂商提供被测设备所涉及的重要数据清单。

c） 检测方法：
1） 通过人工查看和工具验证，检查存储的重要数据是否有保密性和完整性保护措施，是否可通过密码算法保证重要数据的保密性和完整性；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，被测设备可支持使用密码技术保证重要数据存储过程中的保密性和完整性；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.5 重要数据安全防御能力

重要数据安全防御能力测试方法如下：

a） 安全要求：
可使用密码技术保证设备抵御常见的攻击，防止密钥等重要数据泄露，如计时攻击等（T/TAF 217—2024 5.6e））。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备抵御常见攻击所采用密码技术的说明，内容应包含使用的技术名称、原理、用途、何处使用及其实现方式。

c） 检测方法：

1） 查看厂商提供的说明资料，检查是否论证了可采用密码技术抵御常见攻击的技术原理；

2） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，厂商提供的说明资料正确且充分地论证了可采用密码技术抵御常见攻击的技术原理；

2） 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7 计算安全密码应用测试

6.7.1 可信计算环境

可信计算环境测试方法如下：

a） 安全要求：

可使用可信计算技术建立可信计算环境（T/TAF 217—2024 5.7a））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备可信计算环境的说明，说明内容应包括计算环境的功能架构、可信密码模块结构、完整性度量机制、身份标识机制和数据安全保护机制；

4） 厂商应提供被测设备可信计算环境与外部环境的接口说明；

5） 厂商应提供被测设备建立可信计算环境所采用密码技术的说明，说明内容应包含使用的密码技术名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查是否可采用密码技术建立可信计算环境，并验证可信计算环境的完整性度量机制、身份标识机制和数据安全保护机制有效；

2） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，采用密码技术建立可信计算环境，可信计算环境的完整性度量机制、身份标识机制和数据安全保护机制有效；

2） 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7.2 计算完整性保护

计算完整性保护测试方法如下：

a） 安全要求：

可使用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证（T/TAF 217—2024 5.7b））。

b） 预置条件：

1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备中重要可执行程序的范围，以及对程序进行完整性保护和真实性验证的凭据；
4） 厂商应提供被测设备保护可执行程序完整性所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式；
5） 厂商应提供被测设备验证可执行程序来源所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查设备在执行重要可执行程序前是否采用密码技术对其来源真实性和完整性进行保护，并验证保护机制是否有效；
2） 篡改对重要可执行程序来源进行真实性验证的凭据（如数字签名），调用该程序；
3） 篡改用于对重要可执行程序进行完整性保护的凭据（如杂凑值），调用该程序；
4） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，可以采用密码技术对重要可执行程序的完整性和来源的真实性进行保护，保护机制有效；
2） 检测方法步骤 2）中，可执行程序无法通过来源的真实性验证，被测设备提示相应错误信息；
3） 检测方法步骤 3）中，可执行程序的完整性校验失败，被测设备提示相应错误信息；
4） 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.1.3 节要求。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.8 性能测试

6.8.1 可靠性测试

可靠性测试方法如下：

a） 安全要求：
应具有在运行高强度加密、解密算法时不会出现因负载过高而造成不能正常提供服务的情况。
1） 应在运行高强度密码算法时，可正常进行路由转发；
3） 密码算法的使用应不受部署模式影响；
4） 在运行高强度密码算法时，应保证网络层控制能力、应用层控制能力的可用性；
5） 在运行高强度密码算法时，应保证安全防护能力的可用性（T/TAF 217—2024 5.8a））。

b） 预置条件：
1） 按测试环境 3 搭建好测试环境；
2） 选择支持安全强度较高密码算法的相关性能运行环境，如 SHA256/SM3、AES128/SM4 等算法。

c） 检测方法：
1） 设备运行高强度加密算法相关功能，如 IPSec VPN；
2） 验证设备当前配置情况下，是否可正常进行路由转发；
3） 验证设备在不同接口形态下，是否可正常进行路由转发；
4） 验证设备在当前配置情况下，是否可正常进行网络层控制以及应用层控制；

5） 验证设备在当前配置情况下，安全防护能力是否生效。

d） 预期结果：

1） 检测方法步骤 2）中，设备可以正常进行路由转发；

2） 检测方法步骤 3）中，设备可以正常进行路由转发；

3） 检测方法步骤 4）中，设备可以正常进行网络层控制以及应用层控制；

4） 检测方法步骤 5）中，设备安全防护能力可以生效。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.8.2 双机部署测试

双机部署测试方法如下：

a） 安全要求：

1） 应具有在运行高强度加密、解密算法时不会出现因负载过高而造成不能正常提供服务的情况。

2） 双机部署时，如运行高强度密码算法，应保证主备可正常切换（T/TAF 217—2024 5.8a））。

b） 预置条件：

1） 按测试环境 4 搭建好测试环境；

2） 选择支持安全强度较高密码算法的相关性能运行环境，如 SHA256/SM3、AES128/SM4 等算法。

c） 检测方法：

1） 设备主备部署，运行高强度加密算法相关功能，如 IPSec VPN；

2） 验证主机宕机后，业务是否正常切换到备机。

d） 预期结果：

检测方法步骤 2）中，业务正常切换。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.8.3 VPN 吞吐量测试

VPN吞吐量测试方法如下：

a） 安全要求：

运行安全强度较高密码算法时，VPN 吞吐量应满足：

- 百兆防火墙：对于64字节、1400字节的UDP报文，吞吐量应分别不小于8Mbps和35Mbps；
- 千兆防火墙：对于64字节、1400字节的UDP报文，吞吐量应分别不小于25Mbps和400Mbps；
- 万兆防火墙：对于64字节、1400字节的UDP报文，吞吐量应分别不小于220Mbps和5Gbps（T/TAF 217—2024 5.8b））。

b） 预置条件：

1） 按测试环境 2 搭建好测试环境；

2） 选择支持安全强度较高密码算法的相关性能运行环境，如 SHA256/SM3、AES128/SM4 等算法。

c） 检测方法：

两台防火墙配置 IPSec，运行高强度密码算法，测试仪发送 UDP 报文，验证经过防火墙隧道的设备吞吐量。

d） 预期结果：

检测方法步骤 1）中，对应百兆、千兆、万兆相关要求，防火墙吞吐量应满足安全要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.8.4 时延测试

时延测试方法如下：

a） 安全要求：

运行安全强度较高密码算法，时延应满足以下指标要求：

- 百兆防火墙：对于64字节、1400字节的UDP报文，平均时延应均不超过4ms；
- 千兆、万兆防火墙：对于64字节、1400字节的UDP报文，平均时延应均不超过1.5ms（T/TAF 217—2024 5.8b））。

b） 预置条件：

1） 按测试环境 2 搭建好测试环境；

2） 选择支持安全强度较高密码算法的相关性能运行环境，如 SHA256/SM3、AES128/SM4 等算法。

c） 检测方法：

两台防火墙配置 IPSec，运行高强度密码算法，测试仪发送 UDP 报文，验证经过防火墙隧道的报文时延。

d） 预期结果：

检测方法步骤 1）中，对应百兆、千兆、万兆相关要求，防火墙平均时延应满足安全要求。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

附 录 A
（资料性）
重要数据说明

表 A.1 中列举了防火墙设备涉及的重要数据。重要数据包括但不限于身份鉴别信息、访问控制信息、配置信息、远程配置指令、升级数据、告警信息、日志信息、密钥等。

表A.1 防火墙涉及的重要数据示例

序号	重要数据类型	备注
1	访问控制信息	系统访问控制策略、网络访问控制信息、重要信息敏感资源标记等
2	身份鉴别信息	如用户口令等
3	配置信息	系统启动时对程序进行配置的信息，如服务端口、数据库连接信息、线程池信息等
4	远程配置指令	远程配置安全策略等
5	升级数据	特征库、规则文件、系统/软件升级包等
6	告警信息	设备故障信息、安全事件告警信息等
7	日志信息	系统操作审计日志、访问日志、系统安全日志等
8	密钥	私钥、对称密钥等

参 考 文 献

[1] GB/T 20281—2020 信息安全技术 防火墙安全技术要求和测试评价方法
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 37092—2018 信息安全技术 密码模块安全要求
[4] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[5] GM/T 0014—2012 数字证书认证系统密码协议规范
[6] T/TAF 167-2023 网络设备密码应用通用测试方法

电信终端产业协会团体标准

网络设备密码应用测试方法　防火墙设备

T/TAF 330—2026

*

电信终端产业协会发布
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版下载网址：www.taf.org.cn