编号：FGBGJ[2012]2091CPFA-06-1

2012 年国家信息安全专项
适用于工业控制系统的防火墙测评方案

编制：_____

审核：_____

批准：_____

2013-01-28 发布　　2013-02-08 实施

公安部计算机信息系统安全产品质量监督测评中心

目　　录

（本页以下空白）

1. 测评依据

《国家发展改革委办公厅关于组织实施2012年国家信息安全专项有关事项的通知》（发改办高技[2012]2091号）

GB/T 20281-2006 信息安全技术 防火墙技术要求和测试评价方法（第三级）

GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则（EAL3）

2. 检验环境

有多台分别运行不同操作系统的计算机及工业控制设备和模拟设备构成的一个基于TCP/IP以太网和工业控制网的网络检验环境。

2.1. 功能测试环境拓扑结构图

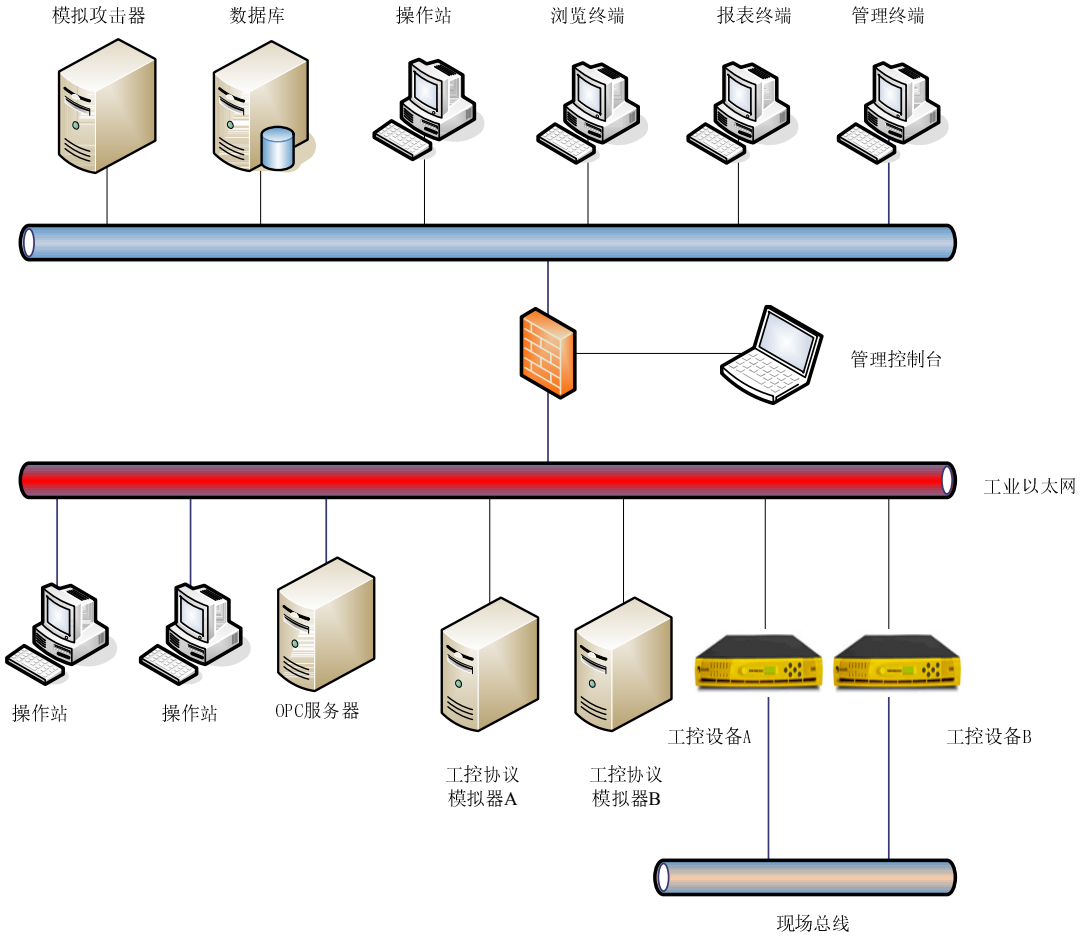

图 1　功能测试环境图

2.2. 性能测试环境拓扑结构图

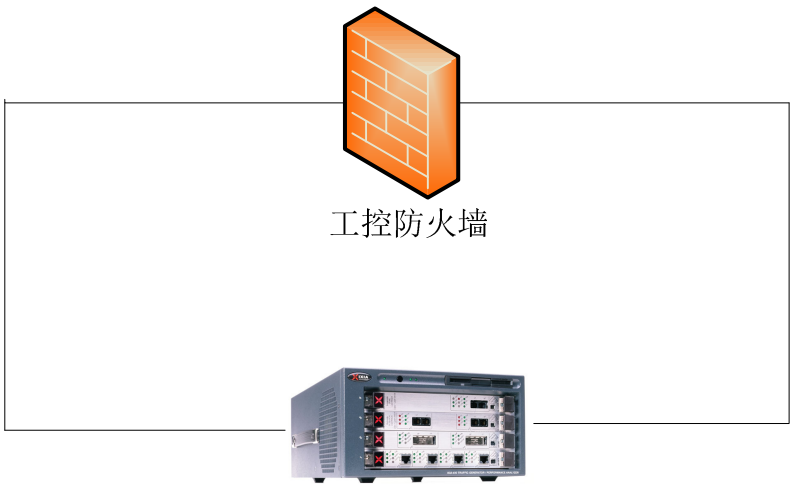

图 2　性能测试环境图

2.3. 测试设备说明

根据上图所述的测试环境结构图，本节对所需的测试设备做一些说明。

表 1 测试设备说明

设备名称	功能	备注
工控设备 A/B	作为被控制的工控设备，需支持不同的主要工控协议	
工控协议模拟器 A/B	采用测试程序模拟各种工控设备	普通 PC
操作站	用于对工控设备进行管理和监控	普通 PC
管理控制台	实现对被测试设备的管理	普通 PC
攻击模拟器	对工控防火墙的外网接口及管理接口进行远程攻击	/
浏览终端、报表终端、数据库等	用于接收工控设备检测数据，并分析报表等	普通 PC
性能测试仪	性能测试	/

3. 检测前准备

3.1. 检测员准备

3.1.1. 知识技能

在进行网络审计系统检测之前，测评员必须学习并熟练掌握如下知识、软件及工具：

⑴ 工业控制防火墙的基本概念、原理和用途；

⑵ TCP/IP 协议；

⑶ 常见的工业控制协议以及工业控制网络的基本结构；

⑷ 工业控制设备模拟器；

⑸ Windows Server 2003、Windows XP Professional 和 Redhat Linux 9.0 等操作系统；IIS 6.0 及操作系统相关服务；

⑹ 通用数据库如 SQLServer、Oracle 等的使用；

⑺ HTTP、FTP、SMTP、POP/POP3、TELNET 等应用层协议和服务的原理及基本配置；

⑻ 流量仿真设备测试仪和入侵流量仿真设备测试仪的使用；

⑼ 以太网络硬件基本结构，会解决基本的网络问题。

3.1.2. 检测环境准备

在检测开始之前，检测员必须做好如下准备：

⑴ 根据 2.3 测试组件说明准备好检测所需要的硬件设备，并为之安装好相应的操作系统及软件；

⑵ 根据 2.1 、2.2 检测环境网络拓扑结构图构建好测试网络，并为之配好相应的 IP 地址等网络属性以及需要的服务；

⑶ 以送检系统分发和操作文档为依据，安装送检的工控防火墙；

⑷ 确认送检系统是否能正常运行，准备工作完成，可以开始检测。

3.1.3. 标准准备

在检测时，检测员尚需准备好如下标准，并通读标准，基本掌握标准内容，以便查询。

⑴ GB/T 20281-2006 信息安全技术 防火墙技术要求和测试评价方法（第三级）

⑵ GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则（EAL3）

⑶ GB 17859-1999 计算机信息系统安全保护等级划分准则

3.1.4. 测试用例的编写

检测员应对照每一条测评依据制定出适合送检产品特点的测试用例。测试用例必须包含用例序号、用例作者、设计日期与具体的输入输出信息，以便减少测试的不确定性，并在追溯错误时能将其再现。

在测试用例编写时，有如下原则与方法可以参考：

⑴ 检测员需仔细研究标准含义，分析在实际情况中可能出现的每一种情况，然后采用等价类划分的方法做较全面的覆盖测试；

⑵ 对具有临界值的测试应尽可能采用边界值的方法进行测试；

⑶ 依据平时检测的经验，可以用错误推测法追加一些测试用例；

⑷ 建议根据业务流的规律，整理每条业务流所对应的标准功能点，依据业务流来进行检测。

3.2. 送检厂商准备

在检测开始之前，送检厂商必须做好如下准备：

⑴ 准备好全部技术文档及资料；

⑵ 准备好送检系统硬件设备及软件安装程序，并在送检之前确认系统版本是否正确，硬件工作是否正常；

⑶ 提供该工控防火墙所支持的测试工控设备；

⑷ 为检测需要，厂商尚需提供本实施细则 4.3 中“文档要求”所规定的全部文档，并准备文档索引表，标明该部分“文档要求”对应所提供的具体文档名或哪本文档的第几页。

4. 测评方法及结果判定

4.1. GB/T 20281-2006 防火墙

4.1.1. 安全功能测试

4.1.1.1. 包过滤

测评依据：

防火墙应具备包过滤功能，具体技术要求如下：

a） 防火墙的安全策略应使用最小安全原则，即除非明确允许，否则就禁止；

b） 防火墙的安全策略应包含基于源IP地址、目的IP地址的访问控制；

c） 防火墙的安全策略应包含基于源端口、目的端口的访问控制；

d） 防火墙的安全策略应包含基于协议类型的访问控制。

e） 防火墙的安全策略可包含基于MAC地址的访问控制；

f） 防火墙的安全策略可包含基于时间的访问控制；

g） 防火墙应支持用户自定义的安全策略，安全策略可以是MAC地址、IP地址、端口、协议类型和时间的部分或全部组合。

文档要求：

提供文档说明产品的默认安全策略，安全策略所支持项目等。

测评方法：

1）检查防火墙的缺省安全策略；

2）配置基于MAC地址的包过滤策略，产生相应的网络会话；

3）配置基于源IP地址、目的IP地址的包过滤策略，产生相应的网络会话；

4）配置基于源端口、目的端口的包过滤策略，产生相应的网络会话；

5）配置基于协议类型的包过滤策略，产生相应的网络会话；

6）配置基于时间的包过滤策略，产生相应的网络会话；

7）配置用户自定义的包过滤策略，过滤条件是2）至6）过滤条件的部分或全部组合，产生相应的网络会话。

预期结果：

1）防火墙采用最小安全原则，即除非明确允许，否则就禁止；

2）防火墙能够根据MAC地址进行过滤；

3）防火墙应能够根据源IP地址、目的IP地址进行过滤；

4）防火墙能够根据源端口、目的端口进行过滤；

5）防火墙能够根据协议类型进行过滤；

6）防火墙能够根据时间进行过滤

7）防火墙能够根据用户定义的策略进行过滤。

4.1.1.2. 状态检测

测评依据：

防火墙应具备状态检测功能。

文档要求：

提供文档说明产品是否具备状态检测功能，支持状态检测的协议类型。

测评方法：

1）配置启动防火墙状态检测模块；

2）配置包过滤策略，允许特定条件的网络会话通过防火墙；

3）产生满足该特定条件的一个完整的网络会话；

4）产生满足该特定条件的网络会话中的不是第一个连接请求SYN包的一个或多个数据包。

预期结果：

1）防火墙依据状态表进行访问控制；

2）满足上述特定条件的一个完整的网络会话能够通过防火墙；

3）满足上述特定条件的网络会话中的不是第一个连接请求SYN包的一个或多个数据包不能通过防火墙。

4.1.1.3. NAT

测评依据：

防火墙应具备NAT功能，具体技术要求如下：

a） 防火墙应支持双向NAT：SNAT和DNAT；

b） SNAT应至少可实现“多对一”地址转换，使得内部网络主机正常访问外部网络时，其源IP地址被转换。

文档要求：

提供文档说明产品是否支持地址转换，以及支持的 NAT。

测评方法：

1）为内部网络用户访问外部网络主机分别设置“多对一”SNAT，检查内部网络中的主机能否通过防火墙访问外部网络中的主机；

2）在内部网络、外部网络内设置协议分析仪，检验数据包在经过防火墙NAT功能前后的源地址、目的地址和包头信息，来验证防火墙地址转换功能的有效性。

预期结果：

1）内部网络主机可通过SNAT访问外部网络主机；

2）外部网络主机能够通过DNAT访问内部服务器；

3）实现“多对一”SNAT，数据包的源地址和目的地址正确转换。

4.1.1.4. IP/MAC 地址绑定

测评依据：

防火墙应具备IP/MAC地址绑定功能，具体技术要求如下：

a） 防火墙应支持自动或管理员手工绑定IP/MAC地址；

b） 防火墙应能够检测IP地址盗用，拦截盗用IP地址的主机经过防火墙的各种访问。

文档要求：

提供文档说明产品是否支持 IP/MAC 地址绑定以及绑定方式，IP 与 MAC 不匹配的处理措施。

测评方法：

1）为防火墙设置IP/MAC地址绑定策略；

2）使用自动绑定或手工绑定功能将内部网络中主机的IP与MAC地址绑定；

3）分别产生正确IP/MAC绑定的会话和盗用IP的会话，检查绑定的有效性。

预期结果：

1）IP/MAC地址能够自动或手工绑定；

2）IP/MAC地址绑定后能够正确执行安全策略，发现IP盗用行为。

4.1.1.5. 动态开放端口

测评依据：

防火墙应具备动态开放端口功能，支持动态开放 OPC 协议端口。

文档要求：

提供文档说明产品的是否支持 OPC 协议，是否支持动态开放 OPC 服务。

测评方法：

1）设置防火墙动态开放端口策略以支持OPC应用；

2）配置一条外网到内网仅允许OPC协议规则，默认禁止其它全部端口。

预期结果：

1）OPC客户端能够正常访问OPC服务，尝试方式其它服务，应该被禁止。

4.1.1.6. 策略路由

测评依据：

具有多个相同属性网络接口（多个外部网络接口、多个内部网络接口）的防火墙应具备策略路由功能，具体技术要求如下：

a） 防火墙应能够根据数据包源目的地址、进入接口、传输层接口或数据包负载内容等参数来设置路由策略；

b） 防火墙应能够设置多个路由表，且每个路由表能包含多条路由信息。

文档要求：

提供文档说明产品是否具有相同属性的网络接口，支持按哪些条件进行策略路由配置。

测评方法：

1）根据源目标地址、进入接口、传输层接口或数据包负载内容等参数配置防火墙策略路由；

2）产生相应的网络会话，检查策略路由的有效性。

预期结果：

1）支持上述至少一种策略路由策略；

2）支持设置多个路由表，每个表包含多条路由信息；

3）防火墙策略路由工作正常。

4.1.1.7. 流量统计

测评依据：

防火墙应具备流量统计功能，具体技术要求如下：

a） 防火墙应能够通过IP地址、网络服务、时间和协议类型等参数或它们的

组合进行流量统计；

b） 防火墙应能够实时或者以报表形式输出流量统计结果。

文档要求：

提供文档说明产品支持按哪些条件进行流量统计，统计数据保存方式。

测评方法：

1）配置防火墙流量统计策略，产生相应的网络流量；

2）检查防火墙能否进行流量统计，并如何输出统计结果。

预期结果：

1）防火墙能够通过IP地址、网络服务、时间和协议类型等参数或它们的组合对流量进行正确的统计；

2）防火墙能够实时或者以报表形式输出流量统计结果。

4.1.1.8. 带宽管理

测评依据：

防火墙应具备带宽管理功能，能够根据安全策略中管理员设定的大小限制客户端占用的带宽。

防火墙应具备带宽管理功能，能够根据安全策略和网络流量动态调整客户端占用的带宽。

文档要求：

提供文档说明产品带宽管理策略，及如果动态调整带宽。

测评方法：

1）配置防火墙带宽管理策略，产生相应的网络流量；

2）从内部网络向外部网络发送流量，流量速率在带宽允许的范围内；

3）从内部网络向外部网络发送流量，使流量的速率超出带宽允许的范围。

预期结果：

1）防火墙能够根据安全策略中管理员设定的大小静态限制客户端占用的带宽；

2）防火墙能够根据安全策略和网络流量动态调整客户端占用的带宽；

3）客户端占用带宽应在限制的范围内。

4.1.1.9. 双机热备

测评依据：

防火墙应具备双机热备功能，具体技术要求如下：

a）防火墙应支持物理设备状态检测。当主防火墙自身出现断电或其他故障时，备防火墙应及时发现并接管主防火墙进行工作；

b）防火墙应具备基于链路状态检测的双机热备功能，当主防火墙直接相连

的链路发生故障而无法正常工作时，备防火墙应及时发现并接管主防火墙进行工作。

文档要求：

提供文档说明产品是否支持双机热备，双机热备实现方式。

测评方法：

1）通过两台防火墙建立双机热备系统，连续产生正常的网络会话；

2）切断主防火墙电源，检查备防火墙是否能够及时发现故障并接管主防火墙进行工作；

3）拔掉内部网络、外部网络或DMZ相连的任意网线，检查备防火墙是否能够及时发现故障并接管主防火墙进行工作。

预期结果：

1）主防火墙电源切断后，备防火墙能够及时故障发现并成功接管主防火墙；

2）拔掉主防火墙相连的网线后，备防火墙能够及时发现故障并成功接管主防火墙。

4.1.1.10. 安全审计

测评依据：

防火墙应具备安全审计功能，具体技术要求如下：

a） 记录事件类型

1） 被防火墙策略允许的从外部网络访问内部网络和防火墙自身的访问请求；

2） 被防火墙策略允许的从内部网络访问外部网络服务的访问请求；

3） 从内部网络、外部网络发起的试图穿越或到达防火墙的违反安全策略的访问请求；

4） 试图登录防火墙管理端口和管理身份鉴别请求；

5） 每次重新启动，包括防火墙系统自身的启动和安全策略重新启动；

6） 所有对防火墙系统时钟的手动修改操作。

b） 日志内容

1） 数据包发生的时间，日期必须包括年、月、日，时间必须包括时、分、秒；

2） 数据包的协议类型、源地址、目标地址、源端口和目标端口等；

3） 指明在管理端口上的认证请求是成功还是失败，若认证请求失败必须记录失败的原因；

c） 日志管理

1） 防火墙应只允许授权管理员访问日志；

2） 防火墙管理员应支持对日志存档、删除和清空的权限；

3） 防火墙应提供能查阅日志的工具，并且只允许授权管理员使用查阅工具；

4） 防火墙应提供对审计事件一定的检索和排序的能力，包括对审计事件以时间、日期、主体ID、客体ID等排序的功能。

5） 防火墙应支持把日志存储和备份在一个安全、永久性的地方；

6） 防火墙应支持只能使用日志管理工具管理日志；

7） 防火墙应支持对日志的统计分析和生成报表的功能；

8） 日志应该可以发送到日志服务器上集中管理；

9） 防火墙日志存储耗尽，防火墙应能采取相应的安全措施，包括向管理员报警、基于策略的最早产生的日志删除和系统工作停止。

文档要求：

提供文档说明产品审计事件的详细范围，日志的管理方式。

测评方法：

1）产生如下事件，检查防火墙是否记录以下日志：

① 从外部网络访问内部网络和安全区域的服务，以及从内部网络访问外部网络、安全区域和防火墙自身；

② 分别从内部网络、外部网络和安全区域发起防火墙安全策略所禁止的数据包；

③ 尝试登录防火墙管理端口，并进行身份鉴别；

④ 重新启动被测防火墙系统；

⑤ 重新启动被测防火墙的安全策略；

⑥ 修改系统时钟；

⑦ 通过IP包仿真器伪造IP数据包，产生协议类型选择为除TCP、UDP和ICMP之外的非标准协议数据包；

⑧ 尝试登录防火墙管理端口，并进行错误操作如输入错误口令；

⑨ 进行多次UDP（如DNS）和ICMP（如ping）协议的访问；

⑩ 进行各项工控协议连接操作。

2）从本地或远程管理端尝试以非授权管理员的身份访问日志；

3）以授权管理员身份登录，查看是否能进行日志查阅、保存、删除和清空的操作；

4）查看防火墙是否能对审计事件进行检索和排序；

5）查看防火墙是否具有将审计记录备份的功能，日志应能够被保存在一个安全、永久的地方；

6）测试防火墙是否只能使用日志管理工具来管理日志；

7）通过在防火墙的本地操作，生成与其存储空间的大小相近的日志文件，模拟存储耗尽的情况；

8）检查防火墙的统计分析和报表生成功能。

预期结果：

1）防火墙准确记录上述各种事件；

2）应记录认证请求是成功还是失败，若为失败，日志应记录失败的原因；

3）应记录事件发生的准确时间：日期包括年、月、日，时间包括时、分、秒；

4）流量日志应包括协议类型、源地址、目标地址、源端口和目标端口等；

5）非授权管理员不能访问日志；

6）授权管理员能进行日志查阅、保存、删除和清空的操作；

7）能对审计事件按时间、主体、客体进行检索和排序；

8）日志安全保存；

9）应只能使用日志管理工具来管理日志，确保日志安全；

10） 日志应能发送到日志服务器上集中管理；

11） 存储耗尽时，能够采取技术要求中的操作；

12） 支持统计分析和报表功能。

4.1.1.11. 管理

测评依据：

防火墙应具备管理功能，具体技术要求如下：

a） 管理安全

1） 支持对授权管理员的口令鉴别方式，且口令设置满足安全要求；

2） 防火墙应在所有授权管理员、可信主机、主机和用户请求执行任何操作之前，对每个授权管理员、可信主机、主机和用户进行唯一的身份识别；

3） 应支持智能卡、USB钥匙等身份鉴别信息载体；

4） 身份鉴别在经过一个可设定的鉴别失败最大次数后，防火墙应终止可信主机或用户建立会话的过程；

5） 防火墙应为每一个规定的授权管理员、可信主机、主机和用户提供一套唯一的为执行安全策略所必需的安全属性；

6） 远程管理过程中，管理端与防火墙之间的所有通讯应加密确保安全；

7） 防火墙向授权管理员提供监控防火墙状态和网络数据流状态的功能；

8） 支持指纹、虹膜等生物特征鉴别方式的管理员身份鉴别；

9） 防火墙应支持管理员权限划分，至少需分为两个部分，可将防火墙管理、安全策略管理或审计日志管理权限分割。

b） 管理方式

1） 防火墙应支持通过console端口进行本地管理；

2） 防火墙应支持通过网络接口进行远程管理。

c） 管理能力

1） 防火墙向授权管理员提供设置和修改安全管理相关的数据参数的功能；

2） 防火墙向授权管理员提供设置、查询和修改各种安全策略的功能；

3） 防火墙向授权管理员提供管理审计日志的功能。

文档要求：

提供文档说明产品所支持的管理方式，采取了哪些措施来保证管理安全，所具备的管理能力范围。

测评方法：

1）查看防火墙的管理方式，是否支持本地管理和远程管理方式，并进行验证；

2）查看防火墙本地和远程管理是否必须通过口令认证；

3）查看防火墙本地和远程管理是否支持生物特征鉴别；

4）查看防火墙是否确保管理员进行操作之前，对管理员、主机和用户等进行唯一的身份识别；

5）在登录过程中输入错误口令，达到防火墙设定的最大失败次数（例如5次）后，查看防火墙是否能够终止可信主机或用户建立会话的过程，并对该失败用户做禁止访问处理；

6）查看防火墙是否提供管理员权限划分功能，并查看防火墙各管理员的权限；

7）通过协议分析仪查看防火墙的管理信息是否安全；

8）查看防火墙的加密是否符合国家密码管理的有关规定。

预期结果：

1）防火墙支持本地和远程两种管理方式；

2）管理员需通过口令验证等身份鉴别措施；

3）对口令设置有一定的强度要求；

4）防火墙支持生物特征鉴别；

5）防火墙确保在管理员进行操作之前，对管理员、主机和用户等进行唯一的身份识别；

6）输入错误口令达到设定的最大失败次数后，防火墙终止可信主机或用户建立会话的过程，并对该失败用户做禁止访问处理；

7）防火墙支持分权管理，对防火墙的不同管理功能进行分割，至少需分为两个部分；

8）远程管理中管理员和防火墙之间的会话安全；

9）防火墙的加密符合国家密码管理的有关规定。

4.1.2. 性能测试

4.1.2.1. 吞吐量

测评依据：

防火墙的吞吐量视不同速率的防火墙有所不同，具体指标要求如下：

a） 防火墙在只有一条允许规则和不丢包的情况下，应达到的吞吐量指标：

1） 对64字节短包，十兆和百兆防火墙应不小于线速的20%，千兆及千兆以上防火墙应不小于线速的35%；

2） 对512字节中长包，十兆和百兆防火墙应不小于线速的70%，千兆及千兆以上防火墙应不小于线速的80%；

3） 对1518字节长包，十兆和百兆防火墙应不小于线速的90%，千兆及千兆以上防火墙应不小于线速的95%；

b） 在添加大数量访问控制规则（不同的200余条）的情况下，防火墙的吞吐量下降应不大于原吞吐量的3%。

文档要求：

提供文档说明该防火墙所支持的速率，该产品的吞吐量。

测评方法：

1）配置测试防火墙只有一条默认允许规则；

2）进行UDP双向吞吐量测试；

3）配置防火墙在200条以上不同访问控制规则；

4）进行UDP双向吞吐量测试。

预期结果：

防火墙的吞吐量性能指标应达到GB/T 20281-2006中5.3.1中规定的最低要求。

4.1.2.2. 延迟

测评依据：

防火墙的延迟视不同速率的防火墙有所不同，具体指标要求如下：

a） 十兆防火墙的最大延迟不应超过1ms；

b） 百兆防火墙的最大延迟不应超过500us；

c） 千兆及千兆以上防火墙的最大延迟不应超过90us；

d） 在添加大数量访问控制规则（不同的200余条）的情况下，防火墙延迟所受的影响应不大于原来的3%。

文档要求：

提供文档说明该防火墙所支持的速率，该产品的延迟。

测评方法：

1）配置测试防火墙只有一条默认允许规则；

2）取GB/T 20281-2006中6.3.2中测得的最大吞吐量，进行延迟测试；

3）配置防火墙在200条以上不同访问控制规则；

4）取GB/T 20281-2006中6.3.2中测得的最大吞吐量，进行延迟测试。

预期结果：

防火墙的延迟性能指标应达到技术要求5.3.2中规定的最低要求。

4.1.2.3. 最大并发连接数

测评依据：

最大并发连接数视不同速率的防火墙有所不同，具体指标要求如下：

a） 十兆防火墙的最大并发连接数应不小于1000个；

b） 百兆防火墙的最大并发连接数应不小于10000个；

c） 千兆及千兆以上防火墙的最大并发连接数应不小于100000个。

文档要求：

提供文档说明该防火墙所支持的速率，该产品的最大并发连接数。

测评方法：

1）配置防火墙允许某种TCP连接；

2）通过专用性能测试设备测试防火墙所能维持的TCP最大并发连接数。

预期结果：

防火墙的最大并发连接数性能指标应达到GB/T 20281-2006中5.3.3中规定的最低要求。

4.1.2.4. 最大连接速率

测评依据：

最大连接速率视不同速率的防火墙有所不同，具体技术要求如下：

a） 十兆防火墙的最大连接速率应不小于每秒500个；

b） 百兆防火墙的最大连接速率应不小于每秒1500个；

c） 千兆及千兆以上防火墙的最大连接速率应不小于每秒5000个。

文档要求：

提供文档说明该防火墙所支持的速率，该产品的最大连接速率。

测评方法：

1）配置防火墙允许某种TCP连接；

2）通过专用性能测试设备测试防火墙的TCP连接速率。

预期结果：

防火墙的最大连接速率性能指标应达到GB/T 20281-2006中5.3.4中规定的最低要求。

4.1.3. 安全性测试

4.1.3.1. 抗渗透

测评依据：

防火墙具备一定的抗攻击渗透能力，具体技术要求如下：

a） 能够抵御Syn Flood、Ping of Death和UDP Flood等基本的拒绝服务攻击，保护自身并防止受保护网络受到攻击；

b） 能够检测和记录端口扫描行为；

c） 能够抵御源IP地址欺骗攻击；

d） 能够抵御IP碎片包攻击；

e） 能够抵御各种典型的拒绝服务攻击和分布式拒绝服务攻击，保护自身并防止受保护网络遭受攻击；

f） 能够检测和记录漏洞扫描行为，包括对受保护网络的扫描；

g） 能够抵御网络扫描行为，不返回扫描信息。

文档要求：

提供文档说明产品能够抵御何种渗透方式及实现技术。

测评方法：

1）采用渗透测试工具或专用性能测试设备，对防火墙进行各种拒绝服务攻击。攻击手段至少包括Syn Flood、UDP Flood、ICMP Flood和Ping of Death；

2）采用端口扫描工具或专业漏洞扫描器，对防火墙及所保护网络进行信息探测；

3）采用渗透测试工具或专用性能测试设备，对防火墙进行源IP地址欺骗、LAND等攻击；

4）采用渗透测试工具或专用性能测试设备，对防火墙进行IP碎片包攻击；

5）检查防火墙能否抵御上述攻击，是否会造成性能下降或崩溃。

预期结果：

1）防火墙工作正常，不同等级产品抵御拒绝服务攻击能力不同，抵御能力应满足GB/T 20281-2006中5.4.1.2、5.4.2.2和5.4.3.2中的技术要求；

2）防火墙工作正常，不同等级产品防御网络扫描的能力不同，应满足GB/T 20281-2006中5.4.1.2、5.4.2.2和5.4.3.2中的技术要求；

3）防火墙工作正常，应抵御IP欺骗攻击和IP碎片包攻击；

4）防火墙性能不应受到明显影响。

4.1.3.2. 恶意代码防御（有则适用）

测评依据：

a）防火墙应具备较强的恶意代码防御能力，能够检测并拦截激活的蠕虫、木马、间谍软件等恶意代码的操作行为；

b） 发现恶意代码后及时向防火墙控制台告警；

c） 至少每月升级一次，支持在线和离线升级；

d）支持对工业控制网恶意代码进行检测和防御。

文档要求：

提供文档说明产品的恶意代码防御机制，采用的杀毒引擎。

测评方法：

略。

预期结果：

参见公安部计算机病毒防治产品检验中心检测结果。

4.1.3.3. 支撑系统

测评依据：

防火墙的底层支撑系统应满足如下技术要求：

a） 确保其支撑系统不提供多余的网络服务；

b） 不含任何导致防火墙权限丢失、拒绝服务和敏感信息泄露的安全漏洞；

c） 防火墙的支撑系统应构建于安全增强的操作系统之上；

d） 防火墙的支撑系统可构建于安全操作系统之上。

文档要求：

提供文档说明所采用的支持系统类型，具有何种安全加固措施。

测评方法：

1）通过随机文档及登录查看，检查防火墙的核心操作系统；

2）通过专业漏洞扫描器，对防火墙进行安全扫描分析。

预期结果：

防火墙支撑系统测试结果应满足GB/T 20281-2006中5.4.1.4、5.4.2.4和5.4.3.4的技术要求。

4.1.3.4. 非正常关机

测评依据：

防火墙在非正常条件（比如掉电、强行关机）关机再重新启动后，应满足如下技术要求：

a） 安全策略恢复到关机前的状态；

b） 日志信息不会丢失；

c） 管理员重新认证。

文档要求：

提供文档说明产品的对非正常关机所采取的保护措施。

测评方法：

1）防火墙正常工作状态中；

2）产生掉电、强行关机等导致的防火墙关闭；

3）重新启动防火墙进行检查。

预期结果：

防火墙的非正常关机测试结果应满足5.4.1.5的技术要求。

4.1.4. 保证要求测试

4.1.4.1. 配置管理

测评依据：

详见GB/T 20281-2006中5.5.2.1、5.5.3.1和5.5.4.1。

文档要求：

提供文档说明产品开放过程中所采用的配置管理系统名称版本，文档清单等。

测评方法：

1） 检查防火墙的版本号，应与对应表示的防火墙产品样本完全对应，没有歧义；

2） 检查防火墙的授权标识，要求开发者所提供的授权标识与所提供给用户的防火墙产品样本完全对应且唯一；

3） 检查防火墙的配置管理系统，并尝试各种操作；

4） 检查防火墙的各种配置管理文件。

预期结果：

防火墙的配置管理测试结果应满足GB/T 20281-2006中5.5.2.1、5.5.3.1和5.5.4.1的技术要求。

4.1.4.2. 交付与运行

测评依据：

详见GB/T 20281-2006中5.5.2.2、5.5.3.2和5.5.4.2。

文档要求：

提供文档说明产品的交付过程、交付安全措施；安装、生成和启动过程。

测评方法：

1） 审查防火墙随机文档，是否能说明防火墙产品的安装、生成和启动的过程；

2） 审查防火墙在连续一周时间内的连续运行情况；

3） 在防火墙配置管理系统中输入错误参数，查看防火墙反应。

预期结果：

防火墙的交付和运行测试结果应满足GB/T 20281-2006中5.5.2.2、5.5.3.2

和5.5.4.2的技术要求。

4.1.4.3. 安全功能开发过程

测评依据：

详见GB/T 20281-2006中5.5.2.3、5.5.3.3和5.5.4.3。

文档要求：

提供文档说明产品的安全功能开发过程、开发环境安全、高层设计、底层设计等。

测评方法：

1） 审查防火墙的安全策略设置指南；

2） 审查防火墙的高层设计描述；

3） 审查防火墙的低层设计描述；

4） 审查防火墙的非形式的一致性证明。

预期结果：

防火墙的开发保证要求的测试结果应满足GB/T 20281-2006中5.5.2.3、5.5.3.3和5.5.4.3的技术要求。

4.1.4.4. 指导性文档

测评依据：

详见GB/T 20281-2006中5.5.2.4、5.5.3.4和5.5.4.4。

文档要求：

提供文档说明产品的管理员指南、用户指南。

测评方法：

1） 审查防火墙的管理员指南；

2） 审查防火墙的用户指南。

预期结果：

防火墙的指南文件测试结果应满足GB/T 20281-2006中5.5.2.4、5.5.3.4和5.5.4.4的技术要求。

4.1.4.5. 生命周期支持

测评依据：

详见GB/T 20281-2006中5.5.2.5和5.5.4.5。

文档要求：

提供文档说明产品的生命周期模型，人员、环境、设备、开发过程和成果管理措施。

测评方法：

1） 检查防火墙的生命周期模型及相关的技术和工具；

2） 检查开发人员的安全管理；

3） 检查开发环境的安全管理；

4） 检查开发设备的安全管理；

5） 检查开发过程和成果的安全管理。

预期结果：

防火墙的测试保证要求的测试结果应满足GB/T 20281-2006中5.5.2.5和5.5.4.5的技术要求。

4.1.4.6. 测试

测评依据：

详见GB/T 20281-2006中5.5.2.6、5.5.3.5和5.5.4.6。

文档要求：

提供文档说明产品的自测报告、测试覆盖分析、测试深度分析。

测评方法：

1） 审查防火墙的自测报告，是否覆盖防火墙全部安全功能；

2） 审查防火墙是否具有整个开发周期的测试报告；

3） 审查开发者提供的测试文档；

4） 审查开发者提供的测试覆盖分析结果；

5） 审查开发者提供的测试深度分析；

6） 审查开发者是否提供了防火墙产品经过独立的第三方测试并通过的证据。

预期结果：

防火墙的测试保证要求的测试结果应满足GB/T 20281-2006中5.5.2.6、5.5.3.5和5.5.4.6的技术要求。

4.1.4.7. 脆弱性评定

测评依据：

详见GB/T 20281-2006中5.5.3.6和5.5.4.7。

文档要求：

提供文档说明产品的脆弱性分析文档。

测评方法：

1） 确认指南性文档，并检查其内容；

2） 通过随机文档，检查开发者在开发过程中是否对防火墙安全机制强度进行分析；

3） 通过随机文档，检查开发者在开发过程中是否对防火墙的脆弱性进行分析；

4） 评估开发者提供的脆弱性分析文档。

预期结果：

防火墙的脆弱性分析的测试结果应满足 GB/T 20281-2006 中 5.5.3.6 和 5.5.4.7 的技术要求。

4.2. 发改办高技[2012]2091 号

4.2.1. 基于白名单策略的访问控制

测评依据：

防火墙应支持基于白名单策略的访问控制，包括网络层和应用层。

文档要求：

提供文档说明产品的访问控制机制。

测评方法：

1）配置开放指定IP、指定端口服务；

2）配置以白名单方式开放指定的工业控制协议、指定开放相应的应用层内容，如开放可执行的命令集、监测参数列表等。

预期结果：

1）通过防火墙能够访问指定开放的服务，不能访问其他IP地址的其它任何服务；

2）能够对工控设备执行白名单中的各项命令和接收白名单中的监测参数列表；不能执行白名单之外的命令和接收白名单之外的监测参数。

4.2.2. 支持多路由协议

测评依据：

防火墙应支持静态路由、（基于源地址、协议或端口、接口等）策略路由。

文档要求：

提供文档说明产品所支持的路由协议。

测评方法：

1）检查厂商申明产品所支持的路由协议类型；

2）检查防火墙是否支持策略路由。

预期结果：

1）防火墙支持静态路由；

2）防火墙应支持策略路由等多路由协议。

4.2.3. 工业控制协议过滤

测评依据：

防火墙应具备深度包检测功能，具体技术要求如下：

a) 防火墙的安全策略应包含Modbus TCP 、ProfiNet或ProfiBus/DP、DNP3.0协议格式检查机制；

b) 防火墙的安全策略应包含Modbus TCP、ProfiNet或ProfiBus/DP、DNP3.0功能码与寄存器检查机制；

d) 防火墙的安全策略应包含OPC的协议格式检查机制；

e）防火墙的安全策略应包含 OPC 的协议完整性检查机制。

文档要求：

提供文档说明产品的所支持的工业控制协议类型，对各种协议所能支持的内容检查范围。

测评方法：

1）分别配置允许和禁止上述各协议的内容要求，如禁止设定的命令；

2）尝试发送异常的协议内容。

预期结果：

防火墙能够基于至少上述各协议的格式检查、内容过滤。

4.2.4. 能够适用于不同工业控制网络应用场景

测评依据：

防火墙至少应支持以下工业控制网络：TCP/IP、ModBus TCP、OPC、DNP3.0、ProfiBus/DP、ProfiNet。

文档要求：

提供文档说明产品所支持的工业控制网络应用场景类型。

测评方法：

1）配置不同工业控制网络的实际网络或模拟环境；

2）在各种场景下，检查防火墙是否能够对各种工业控制协议进行控制。

预期结果：

在各种不同的工业控制网络中，防火墙均能实现其主要防护功能。

4.2.5. 具有高可靠性

测评依据：

防火墙应具有高可靠性，具有要求如下：

a）支持冗余电源；

b） 故障自恢复等；

c）在一定负荷下 72 小时正常运行；

d） 无风扇、支持导轨式或机架式安装。

文档要求：

提供文档说明产品在高可靠性方面所采取的各项措施。

测评方法：

1）检查设备是否支持双电源；

2）尝试破坏设备中部分关键文件，重启设备，检查是否能够自动恢复；

3）模拟一定的网络负荷，持续时间不少于72小时，检查设备是否能够保持正常工作；

4）开箱检查设备，查看是否带有风扇；

5）检查设备是否支持导轨式或机架式安装。

预期结果：

1）设备至少支持双电源以上；

2）设备部分关键文件破坏时能够自恢复；

3）设备至少支持72小时无故障运行；

4）设备应不带风扇，支持导轨式或机架式安装。

4.3. EAL3 级测评

4.3.1. TOE 描述

本次被测产品为 XXX 公司的“XXX 工控防火墙（型号）VX.X”，以下简称“XXX 工控防火墙”。XXX 工控防火墙（型号）VX.X 是一款 XXX，由专用硬件平台及运行于该平台上的软件组成。主要功能包括：数据包过滤、状态检测、地址转换、MAC 绑定、流量统计、带宽管理、双机热备、安全审计、抗渗透等。XXX 工控防火墙（型号）VX.X 提供了 x 个 CONSOLE 口，x 个百/千兆电口，可通过 xx 方式对产品进行管理。

本次评估对象（TOE）仅限于在《XXX 工控防火墙（型号）VX.X 安全目标》中所定义的 TOE 安全功能（TSF），以及构成 TOE 安全功能的接口。其中所有在 TOE 安全功能范围之外的软件、数据库、密码算法自身安全性以及运行 XXX 工控防火墙（型号）VX.X 的所有硬件均不属于本次评估范围。

TOE 软硬件配置信息如下表所示：

项目	描述
产品名称	
产品版本	
产品（系统）形态	软件（ ） 硬件（ ） 固件（ ）
生产集成厂商	
软件运行环境	
硬件配置信息	

4.3.2. 测评证据

序号	证据

序号	证据
1.	XX 工控防火墙（型号）VX.X 安全目标
2.	XX 工控防火墙（型号）VX.X 功能规范
3.	XX 工控防火墙（型号）VX.X 高层设计
4.	XX 工控防火墙（型号）VX.X 对应性分析
5.	XX 工控防火墙（型号）VX.X 配置管理
6.	XX 工控防火墙（型号）VX.X 交付和运行
7.	XX 工控防火墙（型号）VX.X 开发安全
8.	XX 工控防火墙（型号）VX.X 管理员指南
9.	XX 工控防火墙（型号）VX.X 用户指南
10.	XX 工控防火墙（型号）VX.X 测试文档
11.	XX 工控防火墙（型号）VX.X 脆弱性分析
12.	用于测试的 TOE

4.3.3. 测评活动

GB/T 18336 EAL3 测评活动包括：

1) 安全目标评估；
2) 开发活动评估；
3) 交付和运行评估；
4) 配置管理评估；
5) 指导性文档评估；
6) 生命周期支持评估；
7) 测试评估；
8) 脆弱性评估。

4.3.4. 测评判据

评估内容	预期结果
ASE 评估	满足 EAL3 相关要求
ADV_FSP.1	满足 EAL3 相关要求
ADV_HLD.2	满足 EAL3 相关要求

ADV_RCR.1	满足 EAL3 相关要求
ADO_DEL.1	满足 EAL3 相关要求
ADO_IGS.1	满足 EAL3 相关要求
ACM_CAP.3	满足 EAL3 相关要求
ACM_SCP.1	满足 EAL3 相关要求
AGD_ADM.1	满足 EAL3 相关要求
AGD_USR.1	满足 EAL3 相关要求
ALC_DVS.1	满足 EAL3 相关要求
ATE_COV.2	满足 EAL3 相关要求
ATE_DPT.1	满足 EAL3 相关要求
ATE_FUN.1	满足 EAL3 相关要求
ATE_IND.2	满足 EAL3 相关要求
AVA_MSU.1	满足 EAL3 相关要求
AVA_SOF.1	满足 EAL3 相关要求
AVA_VLA.1	满足 EAL3 相关要求

评估活动需满足上表要求，评估最终裁定结果为通过。

4.3.5. 测评内容

4.3.5.1. 安全目标评估

评估子活动包括：

- ST 引言的评估(ASE_INT.1)
- TOE 描述的评估(ASE_DES.1)
- 安全环境的评估(ASE_ENV.1)
- 安全目的的评估(ASE_OBJ.1)
- IT 安全要求的评估(ASE_REQ.1)
- 明确陈述的 IT 安全要求的评估(ASE_SRE.1)
- TOE 概要规范的评估(ASE_TSS.1)
- PP 声明的评估(ASE_PPC.1)

评估证据：

- 开发者应当提供安全目标文档

评估内容：

- ST 引言中应包含 ST 标识信息，该标识应可用于控制和标识 ST 的版本变化，以及与其对应的 TOE 的标识和描述性信息；
- ST 引言中应包含对 ST 概括性描述；
- ST 引言中应包含与 GB/T 18336 的一致性声明，该声明应陈述 TOE 与

GB/T 18336 的一致性，如有与 GB/T 18336 不一致的情况也须声明；

- TOE 描述部分应对概括陈述 TOE 的类型，并从物理和逻辑两方面概述 TOE 的范围和边界；
- TOE 安全环境部分应以 TOE 的预期使用环境为基础分析 TOE 所要保护的资产，标识并解释 TOE 或其环境所保护的资产可能面临的任何已知或假定的威胁；
- TOE 安全环境部分应列出以认为 TOE 是安全的为前提而做出的所有假设；
- TOE 安全环境部分应列出所有 TOE 及其环境必须遵守的组织安全策略，这些策略是由控制 TOE 使用环境的组织制定的；
- ST 的安全目的一节应包括 TOE 安全目的和环境安全目的两部分，并证明安全目的与假设、威胁、组织安全策略之间的对应关系；
- 确认文档描述了安全功能要求和安全保证要求，并对其内容进行了正确的个性化描述，以及组件之间的依赖关系是正确的；
- 确认文档是否存在自定义的安全组件，并判断其正确性；
- 确认文档描述了 TOE 的安全功能和保证措施，并证明其与安全要求之间的对应关系；
- 对于所有用到了概率和置换机制实现的安全功能，应在 ST 中声明其应达到的最低强度级别；
- 确认 ST 包含了与 PP 的符合性声明，未遵循 PP 的 ST 此项可不考虑；
- ST 的各部分的陈述应是一致的。

4.3.5.2. 开发活动评估

评估子活动包括：

- 功能规范评估(ADV_FSP.1)
- 高层设计评估(ADV_HLD.2)
- 表示对应性评估（ADV_RCR.1）

评估证据：

- 开发者应当提供功能规范文档
- 开发者应当提供高层设计文档
- 开发者应当提供对应性分析文档

评估内容：

- 功能规范应以非形式化的语言描述**所有的**安全功能及其外部接口，上下文之间不得有矛盾的地方；
- 功能规范应说明所有安全功能外部接口的用途与使用方法，必要时

还要给出接口操作所可能产生的影响、例外情况和错误信息；

- 高层设计应以非形式化的语言，以子系统的形式描述 TOE 安全功能的结构，以及每个子系统所提供的安全功能，上下文之间不得有矛盾的地方；
- 高层设计需标识出执行 TOE 安全功能所需的所有基础性硬件、固件或软件，并列出由这些硬件、固件或软件实现的支持性保护机制所提供的功能；
- 高层设计应标识出 TOE 安全功能子系统的所有接口，并标识出哪些接口是外部可见的；
- 高层设计应将 TOE 分成与 TSP 相关的子系统和其他子系统来描述；
- 功能规范、高层设计与 ST 文档之间的描述需一致；
- 确认功能规范和高层设计是 TOE 安全功能要求的准确且完备的实例。

4.3.5.3. 交付和运行评估

评估子活动包括：

- 交付评估（ADO_DEL.1）
- 安装、生成和启动评估（ADO_IGS.1）

评估证据：

- 开发者应提供交付文档
- 开发者应提供 TOE 安装、生成和启动相关文档。

评估内容：

- 确认文档描述了将 TOE 交付给最终用户各个环节所采取的安全程序和安全措施；
- 确认文档描述了 TOE 安全安装、生成和启动的所有程序和步骤；
- 结合测试结果确认安装、生成和启动程序最终能够产生安全配置；
- 评估者需进行现场核查。

4.3.5.4. 配置管理评估

评估子活动包括：

- CM 能力评估（ACM_CAP.3）
- CM 范围评估（ACM_SCP.1）

评估证据：

- 开发者应提供用于测试的 TOE；
- 开发者应提供一个 TOE 的参照号；
- 开发者应使用一个配置管理系统；

- 开发者提供的 CM 文档应包括一个配置管理清单和一个配置管理计划。

评估内容：

- 配置管理文档应包括配置项清单和配置管理计划，配置项清单应列出所有组成 TOE 的配置项；
- 配置管理文档中应给出配置项的命名规则，保证配置项清单中标识的配置项的唯一性；
- 确认开发者提交的 TOE 标记了参照号；
- 确认开发者提供的 TOE 参照号，确认 TOE 版本是唯一的，可以被用户识别出。
- 配置管理计划应描述配置管理系统是如何运行的，配置管理系统中应包含所有的配置项，且系统的运行应与配置管理计划中的描述一致；
- 配置管理系统应提供措施使得只能对配置项进行授权改变。
- 评估者需进行现场核查。

4.3.5.5. 指导性文档评估

评估子活动包括：

- 管理员指南评估（AGD_ADM.1）
- 用户指南评估（AGD_USR.1）

评估证据：

- 开发者应提供管理员指南文档；
- 开发者应提供用户指南文档。

评估内容：

- 确认管理员指南文档描述了 TOE 管理员可使用的管理功能和接口；
- 确认管理员指南文档与提交的其他文档保持一致；
- 确认用户指南文档描述了非管理员用户可用的功能和接口；
- 确认用户指南文档描述了用户可访问的安全功能的用法；
- 确认用户指南文档与提交的其他文档保持一致。

4.3.5.6. 生命周期支持评估

评估子活动包括：

- 开发安全评估（ALC_DVS.1）

评估证据：

- 安全目标；

- 开发安全文档；
- 其他交付件，特别是配置管理文件；
- 开发者提供的保证开发安全的执行程序方面的证据。

评估内容：

- 开发安全文档应描述在 TOE 的开发环境中，为保证在 TOE 设计和实现的过程中的机密性和完整性所必需遵守的所有安全制度和规则，所有必需的安全措施；
- 采取的安全措施至少应包括物理上的、过程上的、人员上的和其他安全措施（例如：所有开发机上的逻辑保护）；
- 开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据；
- 评估者需进行现场核查。

4.3.5.7. 测试评估

评估子活动包括：

- 范围评估（ATE_COV.2）
- 深度评估（ATE_DPT.1）
- 功能测试（ATE_FUN.1）
- 独立性测试（ATE_IND.2）

评估证据：

- 开发者应提供用于测试的 TOE；
- 开发者应提供测试文档，包括：对安全功能的测试、测试范围分析、测试深度分析；
- 评估者进行的独立性测试的结果。

评估内容：

- 确认测试文档对安全功能进行了测试；
- 确认测试文档中的测试与功能规范中描述的 TSF 是完全对应的；
- 确认测试文档描述了测试目的、测试步骤、预期结果以及实际结果；
- 检查测试文档中的预期测试结果是否与给出的实际测试结果相一致；
- 确认高层设计中描述的子系统和接口在测试文档中都有相应的测试；
- 检查测试文档中的自测结果是否与独立性测试结果相一致；
- 评估者依据独立设计的测试用例及对开发者测试用例的抽样执行独立性测试，测试要求如表 2；（**具体可根据实际产品的安全功能增加**

或删减有关测试要求）；

表 2 独立性测试要求

序号	安全功能要求	安全功能	备注
1.	FAU_GEN.1 审计数据产生	安全审计功能	如审计日志存储在防火墙上，且能满足审计存储的保证要求，则选“FAU_STG.2 审计数据可用性保证”和“FAU_STG.4 防止审计数据丢失”，不选“FPT_ITC.1 传送过程中 TSF 间的保密性”。
2.	FAU_SAR.1 审计查阅		
3.	FAU_SAR.2 限制审计查阅		
4.	FAU_SAR.3 可选审计查阅		
5.	FAU_STG.2 审计数据可用性保证		
6.	FAU_STG.4 防止审计数据丢失		
7.	FDP_ACC.1 子集访问控制	用户认证功能	
8.	FDP_IFC.1 子集信息流控制	访问控制功能 地址转换功能 抗网络攻击	
9.	FDP_IFF.1 简单安全属性	访问控制功能 地址转换功能 抗网络攻击	
10.	FIA_AFL.1 鉴别失败处理	用户认证功能 系统管理功能	
11.	FIA_ATD.1 用户属性定义	用户管理功能	
12.	FIA_UID.2 任何动作前的用户标识	用户认证功能	
13.	FIA_UAU.2 任何动作前的用户鉴别	用户认证功能	
14.	FIA_UAU.5 多重鉴别机制	用户认证功能	如有两种以上鉴别机制，可以选此组件。
15.	FMT_MOF.1 安全功能行为的管理	用户管理功能 系统管理功能	
16.	FMT_MSA.1 安全属性的管理	用户管理功能 系统管理功能	
17.	FMT_MSA.3 静态属性初始化	系统管理功能	
18.	FMT_MTD.1 TSF 数据的管理	用户管理功能 系统管理功能	
19.	FMT_SMF.1 管理功能规范	用户管理功能 系统管理功能	
20.	FMT_SMR.1 安全角色	用户管理功能	
21.	FPT_ITC.1 传送过程中 TSF 间的保密性	安全审计功能	如审计日志的存储需通过专有的或第三方日志服务器进行，则选择此组件，不选“FAU_STG.2

			审计数据可用性保证”和“FAU_STG.4 防止审计数据丢失”。
22.	FPT_RVM.1 TSP 不可旁路性	用户管理功能 用户认证功能 访问控制功能 系统管理功能 安全审计功能 地址转换功能 抗网络攻击	
23.	FPT_STM.1 可靠的时间戳	系统管理功能	
24.	FTA_MCS.1 多重并发会话的基本限定	访问控制功能	
25.	FTA_SSL.3 TSF 原发会话终止	系统管理功能	
26.	FTP_TRP.1 可信路径	系统管理功能	

4.3.5.8. 脆弱性评估

评估子活动包括：

- 误用评估（AVA_MSU.1）
- TOE 安全功能强度评估（AVA_SOF.1）
- 脆弱性分析（AVA_VLA.1）

评估证据：

- 开发者应提供脆弱性文档；
- 开发者应提供指导性文档；
- 评估者进行的穿透性测试的结果。

评估内容：

- 确认文档对 TOE 相关安全机制的安全功能强度进行了分析；
- 确认文档对 TOE 的脆弱性进行了分析：明显脆弱性有有效的处置方法；说明已标识的脆弱性不能在 TOE 的预期使用环境中被利用，同时通过穿透性测试来进行验证；
- 确认指导性文档描述完备：
  1. 标识了 TOE 所有可能的运行模式（包括失败或操作失败后的运行）及运行后果；
  2. 描述对预期使用环境的所有假设；
  3. 列出对外部安全措施，包括外部程序的、物理的或人员的控制的所有要求。
- 确认依据指导性文档能够安全配置和使用 TOE；
- 确认指导性文档没有误导用户的内容，使用指导性文档能将不安全

状态检测出来；

- 评估者执行穿透性测试，包括口令暴力破解、管理平台安全性测试、未声明端口安全性测试、越权操作、规则有效性、IP 碎片攻击、ARP 脆弱性、源路由攻击及异常协议攻击测试等共 9 个测试项（**具体可根据实际产品的安全功能增加或删减有关测试项**）：

序号	测试项	备注
1	口令暴力破解	
2	管理平台安全性测试	
3	未声明端口安全性测试	
4	越权操作	
5	规则有效性	
6	IP 碎片攻击	
7	ARP 脆弱性	
8	源路由攻击	
9	异常协议攻击测试	

4.3.5.9. 独立性测试

测试目的：

TOE 安全功能执行的正确性。

预期结果：

1. 开发者应提供一个与开发者的安全功能测试中使用的资源相当的合集；
2. 评估者参考开发者提供的测试文档形成抽样子集；如下表：

序号	安全功能	测试用例	备注
1	系统管理功能	用户超时退出 系统时间 数据安全传输	
2	用户管理功能	用户管理	
3	用户认证功能	鉴别失败处理 用户初始登录 初始化配置 用户用户认证	
4	抗网络攻击功能	抗网络攻击	
5	地址转换功能	地址转换	

6	访问控制功能	包过滤 IP/MAC 绑定 流量管理 应用层过滤 会话限制 工业控制协议支持 状态检测表的有效性	
7	安全审计功能	日志记录 日志操作 日志存储 日志传输保护	

根据实际产品的安全功能进行增加

4.3.5.10. 穿透性测试

序号	测试项	测试用例	备注
1.	口令暴力破解	口令暴力破解	
2.	管理平台安全性测试	管理平台 telnet 协议安全性测试 管理平台 ssh 协议安全性测试 管理平台 https 协议安全性测试 Web 管理控制台 SQL 注入攻击 Web 管理控制台跨站（XSS）脚本攻击 Web 管理控制台目录遍历攻击 Web 管理控制台其他漏洞检测	
3.	未声明端口安全性测试	未声明端口安全性测试	
4.	越权操作	用户操作权限限制测试 未授权用户非法访问测试	
5.	规则有效性	规则有效性	
6.	IP 碎片攻击	IP 碎片攻击	
7.	ARP 脆弱性	ARP 脆弱性	
8.	源路由攻击	源路由攻击	
9.	异常协议攻击测试	异常协议攻击测试	

4.3.5.10.1. 口令暴力破解

测试目的：检测 TOE 抵御口令暴力猜测的能力。

预期结果：TOE 能够采取安全措施来防止口令暴力破解攻击。

4.3.5.10.2. 管理平台 telnet 协议安全性测试

测试目的：通过发送 telnet 协议畸形报文验证 TOE 的管理系统能否抵御畸形报文攻击。

预期结果：TOE 的管理系统能够抵御 telnet 协议畸形报文攻击。

4.3.5.10.3. 管理平台 ssh 协议安全性测试

测试目的：通过发送 ssh 协议畸形报文验证 TOE 的管理系统能否抵御畸形报文攻击。

预期结果：TOE 的管理系统能够抵御 ssh 协议畸形报文攻击。

4.3.5.10.4. 管理平台 https 协议安全性测试

测试目的：通过发送 https 协议畸形报文验证 TOE 的管理系统能否抵畸形报文御攻击。

预期结果：TOE 的管理系统能够抵御 https 协议畸形报文攻击。

4.3.5.10.5. Web 管理控制台 SQL 注入攻击

测试目的：检查送测 TOE 的 Web 管理控制台是否存在 SQL 注入漏洞，分析其对 TOE 安全性的影响。

预期结果：送测 TOE 的 Web 管理控制台应能阻止 SQL 注入攻击。

4.3.5.10.6. Web 管理控制台跨站（XSS）脚本攻击

测试目的：检查送测 TOE 的 Web 管理控制台是否能够抵御跨站（XSS）脚本攻击，分析其对 TOE 安全性的影响。

预期结果：送测 TOE 的 Web 管理控制台应能够阻止跨站脚本攻击。

4.3.5.10.7. Web 管理控制台目录遍历攻击

测试目的：检查送测 TOE 的 Web 管理控制台是否存目录遍历漏洞，分析其对 TOE 安全性的影响。

预期结果：Web 管理控制台应能够阻止目录遍历攻击。

4.3.5.10.8. Web 管理控制台其他漏洞检测

测试目的：检查送测 TOE 的 Web 管理控制台是否存源代码信息泄露、代码上传等漏洞，分析其对 TOE 安全性的影响。

预期结果：Web 管理控制台应不存在明显可被利用的其他类型漏洞。

4.3.5.10.9. 未声明端口安全性测试

测试目的：验证 TOE 相关网络接口是否开放了未声明端口及服务。

预期结果：TOE 未开放未声明端口及服务，能够抵御对其保护设备的扫描。

4.3.5.10.10. 用户操作权限限制测试

测试目的：验证 TOE 的访问控制机制，分析访问控制的安全性。检测 TOE 对

合法用户操作权限是否进行了合理控制。

预期结果：TOE 对用户操作权限进行了合理控制。

4.3.5.10.11. 未授权用户非法访问测试

测试目的：检测 TOE 是否能够抵抗用户权限的旁路攻击，防止未登录用户非法访问。

预期结果：TOE 能够抵抗用户权限的旁路攻击，防止未登录用户非法访问。

4.3.5.10.12. 规则有效性

测试目的：检查 TOE 能否准确地根据设定的规则允许或拒绝数据包的通过。

预期结果：TOE 过滤规则不能被旁路。

4.3.5.10.13. IP 碎片攻击

测试目的：检测 TOE 抵御 IP 碎片攻击能力。

预期结果： TOE 具备 IP 分片数据重组能力，并能抵御 IP 碎片攻击。

4.3.5.10.14. ARP 脆弱性

测试目的：验证 TOE 是否能够拒绝不合理的 ARP 数据包。

预期结果： TOE 能够拒绝不同网段 ARP 数据包的通过，能够拒绝不合理的 ARP 数据包。

4.3.5.10.15. 源路由攻击

测试目的：TOE 是否能够抵御源路由攻击。

预期结果：具备源路由攻击的抵御能力。

4.3.5.10.16. 异常协议攻击测试

测试目的：通过发送畸形报文，检测 TOE 抗畸形报文攻击的能力。

预期结果：TOE 能正确处理畸形攻击报文。

4.4. 自主知识产权的检测

测评依据：

对厂家产品代码同业界已有产品代码进行比较，检测厂家产品的自主知识情况。

文档要求：

提供对产品源代码的自主知识产权申明，加盖单位公章。

测评方法及结果判定：

1. 要求厂家以源代码的形式提供产品代码，并提供证明产品代码已经通过 CheckStyle、StyleCop 等代码格式审查工具的检查，格式符合代码相似度检查的要求；
2. 要求厂家在独立干净的机器上进行源代码的编译和生成，并能够对

应到已经部署的软硬件设备上的实际执行代码；

3. 使用 black duck 工具对产品的源代码（关键核心模块）进行对比分析测试，得到相似程度；
4. 相似分析结果应符合自主原创测评指南的要求。