ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20281—2006

信息安全技术
防火墙技术要求和测试评价方法

Information security technology-
Technique requirements and testing and evaluation approaches for firewall products

2006-05-31 发布　　2006-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前鋈言

（略）

信息安全技术
防火墙技术要求和测试评价方法

1 范围

本标准规定了采用“传输控制协议/网际协议（TCP/IP）”的防火墙类信息安全产品的技术要求和测试评价方法。

本标准适用于采用“传输控制协议/网际协议（TCP/IP）”的防火墙类信息安全产品的研制、生产、测试和评估。

2 规范性引用文件

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分：安全（GB/T 5271.8-2001,idt ISO/IEC 2382-8:1998）

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（GB/T 18336.3-2001,idt ISO/IEC 15408-3:1999）

3 术语和定义

GB/T 9387.2、GB/T 18336和GB 17859确立的以及下列术语和定义适用于本标准。

3.1

防火墙 firewall

一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统。

3.2

内部网络 internal network

通过防火墙隔离的可信任区域或保护区域，通常是指单位内部的局域网。

3.3

外部网络 external network

通过防火墙隔离的不可信任区域或非保护区域。

3.4

非军事区 Demilitarized Zone

一个网络对外提供网络服务的部分，受防火墙保护，通过防火墙与内部网络和外部网络隔离，执行与内部网络不同的安全策略，也有的称为安全服务网络（Secure Service Network）。

3.5

安全策略 security policy

有关管理、保护和发布敏感信息的法律、规定和实施细则。

3.6

授权管理员 authorized administrator

具有防火墙管理权限的用户，负责对防火墙的系统配置、安全策略、审计日志等进行管理。

3.7

可信主机 trusted host

赋予权限能够管理防火墙的主机。

3.8

主机 host

一台与防火墙相互作用的机器，它在防火墙安全策略的控制下进行通信。

3.9

用户 user

一个在防火墙安全策略的控制下，通过防火墙访问防火墙的某一个区域的人，此人不具有能影响防火墙安全策略执行的权限。

3.10

吞吐量 throughput

防火墙在不丢包情况下转发数据的能力，一般以所能达到线速的百分比（或称通过速率）来表示。

3.11

延迟 delay

数据帧的最后一个位的末尾到达防火墙内部网络输入端口至数据帧的第一个位的首部到达防火墙外部网络输出端口之间的时间间隔。

3.12

最大并发连接数 maximum concurrent TCP connection capacity

防火墙所能保持的最大TCP并发连接数量。

3.13

最大连接速率 maximum TCP connection establishment rate

防火墙在单位时间内所能建立的最大TCP连接数，一般是每秒的连接数。

4 符号和缩略语

DMZ	非军事区	Demilitarized Zone
DNAT	目的网络地址转换	Destination NAT
DNS	域名系统	Domain Name System
FTP	文件传输协议	File Transfer Protocol
HTTP	超文本传输协议	Hypertext Transfer Protocol
ICMP	网间控制报文协议	Internet Control Messages Protocol
IDS	入侵检测系统	Intrusion Detection System
IP	网际协议	Internet Protocol
NAT	网络地址转换	Network Address Translation
POP3	邮局协议3	Post Office Protocol 3
PBR	策略路由	Policy-based Routing
SMTP	简单邮件传送协议	Simple Mail Transfer Protocol
SNAT	源网络地址转换	Source IP NAT
SSN	安全服务网络	Secure Service Network
STP	生成树协议	Spanning Tree Protocol
TCP	传输控制协议	Transport Control Protocol
UDP	用户数据报协议	User Datagram Protocol
URL	统一资源定位器	Uniform Resource Locator
USB	通用串行总线	Universal Serial Bus

VLAN	虚拟局域网	Virtual Local Area Network
VPN	虚拟专用网	Virtual Private Network
VRRP	虚拟路由器冗余协议	Virtual Router Redundancy Protocol

5 技术要求

5.1 总体说明

5.1.1 技术要求分类

本标准将防火墙通用技术要求分为功能、性能、安全和保证要求四个大类。其中，功能要求是对防火墙产品应具备的安全功能提出具体的要求，包括包过滤、应用代理、内容过滤、安全审计和安全管理等；性能要求对防火墙产品应达到的性能指标作出规定，例如吞吐量、延迟、最大并发连接数和最大连接速率；安全要求是对防火墙自身安全和防护能力提出具体的要求，例如抵御各种网络攻击；保证要求则针对防火墙开发者和防火墙自身提出具体的要求，例如管理配置、交付与操作、指南文件等。

5.1.2 安全等级

本标准依据GB 17859和GB/T 18336.3，并根据国内测评认证机构、测评技术和我国防火墙产品开发现状，对防火墙产品进行安全等级划分。安全等级分为一级、二级、三级三个逐级提高的级别，功能强弱、安全强度和保证要求高低是等级划分的具体依据。安全等级突出安全特性，性能高低不作为等级划分依据。

5.2 功能要求

5.2.1 一级产品功能要求

5.2.1.1 功能要求列表

一级产品的功能要求由表1所列项目组成。

表1 一级产品功能要求细目

功能分类	功能项目要求
包过滤	支持默认禁止原则。
	支持基于IP地址的访问控制。
	支持基于端口的访问控制。
	支持基于协议类型的访问控制。
应用代理	支持应用层协议代理。
NAT	支持双向NAT。
流量统计	支持根据IP地址、协议、时间等参数对流量进行统计。
	支持统计结果的报表形式输出。
安全审计	支持记录来自外部网络的被安全策略允许的访问请求。
	支持记录来自内部网络和DMZ的被安全策略允许的访问请求。
	支持记录任何试图穿越或到达防火墙的违反安全策略的访问请求。
	支持记录防火墙管理行为。
	审计记录内容。
	支持日志的访问授权。
	支持日志的管理。

	提供日志管理工具。
管理	支持对授权管理员的口令鉴别方式。
	支持对授权管理员、可信主机、主机和用户进行身份鉴别。
	支持本地和远程管理。
	支持设置和修改安全管理相关的数据参数。
	支持设置、查询和修改安全策略。
	支持管理审计日志。

5.2.1.2 包过滤

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。

5.2.1.3 应用代理

应用代理型和复合型防火墙应具备应用代理功能，且应至少支持HTTP、FTP、TELNET、POP3和SMTP等协议的应用代理。

5.2.1.4 NAT

包过滤型和复合型防火墙应具备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；

c） DNAT应至少可实现“一对多”地址转换，将DMZ的IP地址映射为外部网络合法IP地址，使外部网络主机通过访问映射地址实现对DMZ服务器的访问。

5.2.1.5 流量统计

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。

5.2.1.6 安全审计

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、DMZ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和DMZ访问外部网络服务的访问请求；

3） 从内部网络、外部网络和DMZ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。

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。

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。

5.2.1.7 管理

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。

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。

5.2.2 二级产品功能要求

5.2.2.1 功能要求列表

二级产品除需满足一级产品的功能要求外，还需具有如表2所示的功能要求。

表2 二级产品功能要求细目

功能分类	功能项目要求
包过滤	支持基于MAC地址的访问控制。
	支持基于时间的访问控制。
	支持基于用户自定义安全策略的访问控制。
状态检测	支持基于状态检测技术的访问控制。
深度包检测	支持基于URL的访问控制。
	支持基于电子邮件信头的访问控制。
应用代理	支持应用层协议代理。
NAT	支持动态NAT。
IP/MAC地址绑定	支持IP/MAC地址绑定。
	支持检测IP地址盗用。
动态开放端口	支持FTP的动态端口开放。
策略路由	支持根据数据包信息来设置路由策略。
	支持设置多个路由表。
带宽管理	支持客户端占用带宽大小限制。

双机热备	支持物理设备状态检测。
	支持VRRP和STP协议。
负载均衡	支持将网络负载均衡到多台服务器。
安全审计	支持记录对防火墙系统自身的操作。
	支持记录在防火墙管理端口上的认证请求。
	支持对日志事件和防火墙所采取的相应措施的描述。
	支持日志记录存储和备份的安全。
	支持日志管理工具管理日志。
	支持日志的统计分析和报表生成。
	支持日志的集中管理。
管　理	支持智能卡、USB钥匙等身份鉴别信息载体。
	支持鉴别失败处理。
	支持授权管理员、可信主机、主机和用户的唯一安全属性。
	支持远程管理安全。
	支持防火墙状态和网络数据流状态监控。

5.2.2.2 包过滤

防火墙应具备包过滤功能，具体技术要求如下：

a） 防火墙的安全策略可包含基于MAC地址的访问控制；

b） 防火墙的安全策略可包含基于时间的访问控制；

c） 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。

5.2.2.3 状态检测

防火墙应具备状态检测功能。

5.2.2.4 深度包检测

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基于URL的访问控制；

b） 防火墙的安全策略应包含基于电子邮件中的Subject、To、From域等进行的访问控制。

5.2.2.5 应用代理

应用代理型和复合型防火墙应具备DNS协议的应用代理。

5.2.2.6 NAT

包过滤型和复合型防火墙应具备NAT功能，具体技术要求如下：

a） 防火墙应支持动态SNAT技术，实现“多对多”的SNAT；

b） 防火墙应支持动态DNAT技术，实现“多对多”的DNAT。

5.2.2.7 IP/MAC 地址绑定

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。

5.2.2.8 动态开放端口

防火墙应具备动态开放端口功能，支持主动模式和被动模式的FTP。

5.2.2.9 策略路由

具有多个相同属性网络接口（多个外部网络接口、多个内部网络接口或多个 DMZ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。

5.2.2.10 带宽管理

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。

5.2.2.11 双机热备

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） 在路由模式下，防火墙可支持VRRP协议；

c） 在透明模式下，防火墙可支持STP协议。

5.2.2.12 负载均衡

防火墙应具备负载均衡功能，能够根据安全策略将网络流量均衡到多台服务器上。

5.2.2.13 安全审计

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） 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；

2） 所有对防火墙系统时钟的手动修改操作。

b） 日志内容

1） 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；

2） 对日志事件和防火墙采取的相应措施进行详细的描述。

c） 日志管理

1） 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；

2） 防火墙应支持只能使用日志管理工具管理日志；

3） 防火墙应支持对日志的统计分析和生成报表的功能；

4） 日志应该可以发送到日志服务器上集中管理。

5.2.2.14 管理

防火墙应具备安全管理功能，具体技术要求如下：

a） 应支持智能卡、USB钥匙等身份鉴别信息载体；

b） 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；

c） 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；

d） 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；

e） 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。

5.2.3 三级产品功能要求

5.2.3.1 功能要求列表

三级产品除需满足一、二级产品的功能要求外，还需具有如表3所示的功能要求。

表3 三级产品功能要求细目

功能分类	功能项目要求
深度包检测	支持基于文件类型的访问控制。
	支持基于用户的访问控制。
	支持基于关键字的访问控制。
应用代理	支持透明应用代理。
动态开放端口	支持以H.323协议建立视频会议。
	支持SQL*NET数据库协议。
	支持VLAN。
带宽管理	支持动态客户端带宽管理。
双机热备	支持链路状态检测的双机热备。
负载均衡	支持集群工作模式的负载均衡。
VPN	支持IPSec协议。
	支持建立“防火墙至防火墙”和“防火墙至客户机”两种形式的VPN。
	支持VPN认证。
	加密算法和验证算法符合国家密码管理的有关规定。
协同联动	支持与其它安全产品的协同联动。
	支持联动安全产品的身份鉴别。
安全审计	支持记录协同联动响应行为事件。
	支持日志存储耗尽处理机制。
管　理	支持生物特征鉴别方式。
	支持管理员权限划分。

5.2.3.2 深度包检测

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基于文件类型的访问控制；

b） 防火墙的安全策略应包含基于用户的访问控制；

c） 防火墙的安全策略可包含基于关键字的访问控制，对HTTP网页数据和和电子邮件正文数据进行检查。

5.2.3.3 应用代理

应用代理型和复合型防火墙应具备透明应用代理功能，支持HTTP、FTP、TELNET、SMTP、POP3和DNS等协议。

5.2.3.4 动态开放端口

防火墙应具备动态开放端口功能，具体技术要求如下：

a） 防火墙应支持以H.323协议建立视频会议；

b） 防火墙应支持SQL*NET数据库协议；

c） 防火墙应支持VLAN协议。

5.2.3.5 带宽管理

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。

5.2.3.6 双机热备

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。

5.2.3.7 负载均衡

防火墙应具备基于集群工作模式的负载均衡功能，使得多台防火墙能够协同工作均衡网络流量。

5.2.3.8 VPN

防火墙可具备VPN功能，具体技术要求如下：

a） 防火墙应支持以IPSec协议为基础构建VPN；

b） 防火墙应支持建立“防火墙至防火墙”和“防火墙至客户机”两种形式的VPN；

c） 防火墙应支持预共享密钥和X.509数字证书两种认证方式来进行VPN认证；

d） 防火墙所使用的加密算法和验证算法应符合国家密码管理的有关规定。

5.2.3.9 协同联动

防火墙应具备与其它安全产品的协同联动功能（例如与IDS），具体技术要求如下：

a） 防火墙应按照一定的安全协议与其它安全产品协同联动，并支持手工与自动方式来配置联动策略；

b） 防火墙应在协同联动前对与其联动的安全产品进行身份鉴别。

5.2.3.10 安全审计

防火墙应具备安全审计功能，具体技术要求如下：

a） 防火墙应记录协同联动响应行为事件；

b） 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。

5.2.3.11 管理

防火墙应具备管理功能，具体要求如下：

a） 支持指纹、虹膜等生物特征鉴别方式的管理员身份鉴别；

b） 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。

5.3 性能要求

5.3.1 吞吐量

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%。

5.3.2 延迟

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%。

5.3.3 最大并发连接数

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。

5.3.4 最大连接速率

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。

5.4 安全要求

5.4.1 一级产品安全要求

5.4.1.1 安全要求列表

一级产品的安全要求由表1所列项目组成。

表4 一级产品安全要求细目

安全分类	安全要求
抗渗透	抵御各种基本的拒绝服务攻击。
	检测和记录端口扫描行为。
	抵御源IP地址欺骗攻击。
	抵御IP碎片包攻击。
恶意代码防御	拦截典型木马攻击行为。
支撑系统	支撑系统不提供多余的网络服务。
	支撑系统应不含任何高、中风险安全漏洞。
非正常关机	安全策略恢复到关机前的状态。
	日志信息不会丢失。
	管理员重新认证。

5.4.1.2 抗渗透

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。

5.4.1.3 恶意代码防御

防火墙应具备基本的恶意代码防御能力，能够拦截典型的木马攻击行为。

5.4.1.4 支撑系统

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。

5.4.1.5 非正常关机

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。

5.4.2 二级产品安全要求

5.4.2.1 安全要求列表

二级产品除需满足一级产品的安全要求外，还需具有如表5所示的安全要求。

表5 二级产品安全要求细目

安全分类	安全要求
抗渗透	抵御各种典型的拒绝服务攻击。
	检测和记录漏洞扫描行为。
	拦截典型邮件炸弹工具发送的垃圾邮件。
恶意代码防御	检测并拦截激活的蠕虫、木马、间谍软件等恶意代码的行为。
支撑系统	构建于安全增强的操作系统之上。

5.4.2.2 抗渗透

防火墙应具备较强的抗攻击渗透能力，具体技术要求如下：

a） 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；

b） 能够检测和记录漏洞扫描行为，包括对受保护网络的扫描；

c） 拦截典型邮件炸弹工具发送的垃圾邮件。

5.4.2.3 恶意代码防御

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。

5.4.2.4 支撑系统

防火墙的支撑系统应构建于安全增强的操作系统之上。

5.4.3 三级产品安全要求

5.4.3.1 安全要求列表

三级产品除需满足一、二级产品的安全要求外，还需具有如表6所示的安全要求。

表6 三级产品安全要求细目

安全分类	安全要求
抗渗透	能够抵御网络扫描行为，不返回扫描信息。
	支持黑名单或特征匹配等方式的垃圾邮件拦截策略配置。
恶意代码防御	检测并拦截被HTTP网页和电子邮件携带的恶意代码。
	恶意代码检测告警。
支撑系统	构建于安全操作系统之上。

5.4.3.2 抗渗透

防火墙应具备很强的抗攻击渗透能力，具体技术要求如下：

a） 能够抵御网络扫描行为，不返回扫描信息；

b） 支持黑名单或特征匹配等方式的垃圾邮件拦截策略配置。

5.4.3.3 恶意代码防御

防火墙应具备很强的恶意代码防御能力，具体技术要求如下：

a） 检测并拦截被HTTP网页和电子邮件携带的恶意代码；

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。

5.4.3.4 支撑系统

防火墙的支撑系统可构建于安全操作系统之上。

5.5 保证要求

5.5.1 说明

保证要求采用增量描述方法。通常，二级产品的保证要求应包括一级产品的保证要求，三级产品的保证要求应包括一级和二级产品的保证要求；在某些项目，高等级产品的保证要求比低等级产品的保证要求更为严格，则不存在增量的关系。

5.5.2 一级产品保证要求

5.5.2.1 配置管理

配置管理应满足如下要求：

a） 开发者应为防火墙产品的不同版本提供唯一的标识；

b） 开发者应针对不同用户提供唯一的授权标识；

c） 配置项应有唯一的标识。

5.5.2.2 交付与运行

交付与运行应满足如下要求：

a） 评估者应审查开发者是否提供了文档说明防火墙的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程；

b） 防火墙运行稳定；

c） 对错误输入的参数，不应导致防火墙出现异常，且给出提示信息。

5.5.2.3 安全功能开发过程

5.5.2.3.1 功能设计

功能设计应满足如下要求：

a） 功能设计应当使用非形式化风格来描述防火墙安全功能与其外部接口；

b） 功能设计应当是内在一致的；

c） 功能设计应当描述使用所有外部防火墙安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节；

d） 功能设计应当完整地表示防火墙安全功能；

e） 功能设计应是防火墙安全功能要求的精确和完整的示例。

5.5.2.3.2 表示对应性

开发者应在防火墙安全功能表示的所有相邻对之间提供对应性分析，具体要求如下：

a） 防火墙各种安全功能表示（如防火墙功能设计、高层设计、低层设计、实现表示）之间的对应性是所提供的抽象防火墙安全功能表示要求的精确而完整的示例；

b） 防火墙安全功能在功能设计中进行细化，抽象防火墙安全功能表示的所有相关安全功能部分，在具体防火墙安全功能表示中应进行细化。

5.5.2.4 指导性文档

5.5.2.4.1 管理员指南

开发者应提供供系统管理员使用的管理员指南，该指南应包括如下内容：

a） 防火墙可以使用的管理功能和接口；

b） 怎样安全地管理防火墙；

c） 对一致、有效地使用安全功能提供指导；

d） 在安全处理环境中应进行控制的功能和权限；

e） 所有对与防火墙的安全操作有关的用户行为的假设；
f） 所有受管理员控制的安全参数，如果可能，应指明安全值；
g） 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；
h） 所有与系统管理员有关的 IT 环境的安全要求；
i） 怎样配置防火墙的指令；
j） 应描述在防火墙的安全安装过程中，可能要使用的所有配置选项。

5.5.2.4.2 用户指南

开发者应提供供系统用户使用的用户指南，该指南应包括如下内容：
a） 防火墙的非管理用户可使用的安全功能和接口；
b） 防火墙提供给用户的安全功能和接口的用法；
c） 用户可获取但应受安全处理环境控制的所有功能和权限；
d） 防火墙安全操作中用户所应承担的职责；
e） 与用户有关的 IT 环境的所有安全要求；
f） 使用防火墙提供的安全功能的指导。

5.5.2.5 生命周期支持

开发者所提供的信息应满足如下要求：
a） 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；
b） 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温室度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料；
c） 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；
d） 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录，若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料。

5.5.2.6 测试

5.5.2.6.1 范围

开发者应提供测试覆盖分析结果，且该测试文档中所标识的测试与安全功能设计中所描述的安全功能对应。

5.5.2.6.2 功能测试

功能测试应满足如下要求：
a） 测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果；
b） 评估测试计划应标识要测试的安全功能，并描述测试的目标；
c） 评估测试过程应标识要执行的测试，应描述每个安全功能的测试概况（这些概况包括对其它测试结果的顺序依赖性）；
d） 评估期望的测试结果应表明测试成功后的预期输出；
e） 评估实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.5.3 二级产品保证要求

5.5.3.1 配置管理

5.5.3.1.1 配置管理能力

配置管理能力应满足如下要求：
a） 开发者应使用配置管理系统并提供配置管理文档，且具备全中文操作界面、易于使用和支持在线帮助，以及为防火墙产品的不同版本提供唯一的标识；

b） 配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项；

c） 配置管理文档应包括配置清单、配置管理计划。配置清单用来描述组成防火墙的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致；

d） 配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.5.3.1.2 配置管理范围

防火墙配置管理范围，应将防火墙的实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。为此要求：

a） 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；

b） 文档应描述配置管理系统是如何跟踪这些配置项的；

c） 文档还应提供足够的信息表明达到所有要求。

5.5.3.1.3 管理配置接口

防火墙应提供各个管理配置项接口，并包括防火墙使用的外部网络的服务项目。

5.5.3.2 交付与运行

交付与运行应满足如下要求：

a） 开发者应使用一定的交付程序交付防火墙；

b） 开发者应使用物理文档描述交付过程；

c） 开发者交付的文档应说明在给用户方交付防火墙的各版本时，为维护安全所必需的所有程序。

5.5.3.3 安全功能开发过程

5.5.3.3.1 高层设计

开发者所提供的信息应满足如下要求：

a） 高层设计应采用非形式化的表示；

b） 高层设计应当是内在一致的；

c） 防火墙高层设计应当描述每一个防火墙安全功能子系统所提供的安全功能，提供了适当的体系结构来实现防火墙安全功能要求；

d） 防火墙的高层设计应当以子系统的观点来描述防火墙安全功能的结构，定义所有子系统之间的相互关系，并把这些相互关系将适当地作为数据流、控制流等的外部接口来表示；

e） 高层设计应当标识防火墙安全功能要求的任何基础性的硬件、固件和/或软件，并且通过支持这些硬件、固件或软件所实现的保护机制，来提供防火墙安全功能表示。

5.5.3.4 指导性文档

5.5.3.4.1 管理员指南

管理员指南应满足如下要求：

a） 对于应该控制在安全环境中的功能和特权，管理员指南应有警告；

b） 管理员指南应说明两种类型功能之间的差别：一种是允许管理员控制安全参数，而另一种是只允许管理员获得信息；

c） 管理员指南应描述管理员控制下的所有安全参数；

d） 管理员指南应充分描述与安全管理相关的详细过程；

e） 管理员指南应与提交给测试、评估和认证的其它文件一致。

5.5.3.4.2 用户指南

用户指南应满足如下要求：

a） 对于应该控制在安全处理环境中的功能和特权，用户指南应有警告；

b） 用户指南应与提交给测试、评估和认证的其它文件一致。

5.5.3.5 测试

5.5.3.5.1 范围

评估测试文档中所标识的测试应当完整。

5.5.3.5.2 深度测试

开发者提供的测试深度分析应说明测试文档中所标识的对安全功能的测试，以表明该安全功能和高层设计是一致的。

5.5.3.5.3 独立性测试

开发者应提供用于测试的产品，且提供的产品适合测试。

5.5.3.6 脆弱性评定

5.5.3.6.1 指南检查

开发者提供的指南性文档应满足如下要求：

a） 指南性文档应确定对防火墙的所有可能的操作方式（包括失败和操作失误后的操作），确定它们的后果，并确定对于保持安全操作的意义；

b） 指南性文档应列出所有目标环境的假设以及所有外部安全措施（包括外部程序的、物理的或人员的控制）的要求；

c） 指南性文档应完整、清晰、一致、合理。

5.5.4 三级产品保证要求

5.5.4.1 配置管理

5.5.4.1.1 配置管理自动化

配置管理应满足如下要求：

a） 开发者应使用配置管理系统，并提供配置管理计划；

b） 配置管理系统应确保只有已授权开发人员才能对防火墙产品实现进行修改，并支持防火墙基本配置项的生成；

c） 配置管理计划应描述在配置管理系统中使用的工具软件。

5.5.4.1.2 配置管理能力

开发者所提供的信息应满足如下要求：

a） 配置管理系统应支持防火墙基本配置项的生成；

b） 配置管理文档应包括接受计划。在接受计划中，应描述对修改过或新建的配置项进行接受的程序。

5.5.4.1.3 配置管理范围

开发者提供的配置管理支持文件应包含以下内容：

a） 问题跟踪配置管理范围，除防火墙配置管理范围描述的内容外，要求特别强调对安全缺陷的跟踪；

b） 开发工具配置管理范围，除问题跟踪配置管理范围所描述的内容外，要求特别强调对开发工具和相关信息的跟踪。

5.5.4.2 交付与运行

交付与运行应满足如下要求：

a） 开发者交付的文档应包含产品版本变更控制的版本和版次说明、实际产品版本变更控制的版本和版次说明、监测防火墙程序版本修改说明；

b） 开发者交付的文档应包含对试图伪装成开发者向用户发送防火墙产品行为的检测方法。

5.5.4.3 安全功能开发过程

5.5.4.3.1 功能设计

开发者所提供的功能规范应当包括防火墙安全功能基本原理的完整表示。

5.5.4.3.2 安全功能实现

开发者所提供的信息是否满足如下要求：

a） 开发者应当为选定的防火墙安全功能子集提供实现表示；

b） 开发者应当为整个防火墙安全功能提供实现表示；

c） 实现表示应当无歧义地定义一个详细级别的防火墙安全功能，该防火墙安全功能的子集无须选择进一步的设计就能生成；

d） 实现表示应当是内在一致的。

5.5.4.3.3 低层设计

开发者所提供的防火墙安全功能的低层设计应满足如下要求：

a） 低层设计的表示应当是非形式化的；

b） 低层设计应当是内在一致的；

c） 低层设计应当以模块术语描述防火墙安全功能；

d） 低层设计应当描述每一个模块的目的；

e） 低层设计应当以所提供的安全功能性和对其它模块的依赖性术语定义模块间的相互关系；

f） 低层设计应当描述如何提供每一个防火墙安全策略强化功能；

g） 低层设计应当标识防火墙安全功能模块的所有接口；

h） 低层设计应当标识防火墙安全功能模块的哪些接口是外部可见的；

i） 低层设计应当描述防火墙安全功能模块所有接口的目的与方法，适当时，应提供影响、例外情况和错误信息的细节；

j） 低层设计应当描述如何将防火墙分离成防火墙安全策略加强模块和其它模块。

5.5.4.3.4 安全策略模型

开发者所提供的信息应满足如下要求：

a） 开发者应提供一个基于防火墙安全策略子集的安全策略模型；

b） 开发者应阐明功能规范和防火墙安全策略模型之间的对应性；

c） 安全策略模型应当是非形式化的；

d） 安全策略模型应当描述所有可以模型化的安全策略模型的规则与特征；

e） 安全策略模型应当包括一个基本原理，即阐明该模型对于所有可模型化的安全策略模型来说，是与其一致的，而且是完整的；

f） 安全策略模型和功能设计之间的对应性阐明应当说明，所有功能规范中的安全功能对于安全策略模型来说，是与其一致，而且是完整的。

5.5.4.4 指导性文档

5.5.4.4.1 管理员指南

管理员指南应满足如下要求：

a） 管理员指南应描述各类需要执行管理功能的安全相关事件，包括在安全功能控制下改变实体的安全特性；

b） 管理员指南应包括安全功能如何相互作用的指导。

5.5.4.4.2 用户指南

用户指南应描述用户可见的安全功能之间的相互作用。

5.5.4.5 生命周期支持

5.5.4.5.1 生命周期模型

开发者所提供的生命周期定义文件中应包含以下内容：

a） 开发者定义的生命周期模型，要求开发者应建立用于开发和维护防火墙的生命周期模型。该模型应对防火墙开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护防火墙的模型。

b） 标准生命周期模型，要求开发者应建立标准化的、用于开发和维护防火墙的生命周期模型。该模型应对防火墙开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护防火墙的模型，解释选择该模型的原因，解释如何用该模型来开发和维护防火墙，以及阐明与标准化的生命周期模型的相符性。

c） 可测量的生命周期模型，要求开发者应建立标准化的、可测量的、用于开发和维护防火墙的生命周期模型，并用此模型来衡量防火墙的开发。该模型应对防火墙开发和维护提供必要的控制。开发者所提供的生命周期定义文档应描述用于开发和维护防火墙的模型，包括针对该模型衡量防火墙开发所需的算术参数和/或度量的细节。生命周期定义文档应解释选择该模型的原因，解释如何用该模型来开发和维护防火墙，阐明与标准化的可测量的生命周期模型的相符性，以及提供利用标准化的可测量的生命周期模型来进行防火墙开发的测量结果。

5.5.4.5.2 工具和技术

开发者所提供的信息应满足如下要求：

a） 明确定义的开发工具，要求开发者应标识用于开发防火墙的工具，并且所有用于实现的开发工具都必须有明确定义。开发者应文档化已选择的依赖实现的开发工具的选项，并且开发工具文档应明确定义实现中每个语句的含义，以及明确定义所有基于实现的选项的含义；

b） 遵照实现标准-应用部分，除明确定义的开发工具的要求外，要求开发者应描述所应用部分的实现标准；

c） 遵照实现标准-所有部分，除遵照实现标准-应用部分的要求外，要求开发者应描述防火墙所有部分的实现标准。

5.5.4.6 测试

5.5.4.6.1 功能测试

功能测试应满足如下要求：

a） 实际测试结果应表明每个被测试的安全功能按照规定进行运作；

b） 提供防火墙在整个开发周期内各个阶段的测试报告。

5.5.4.6.2 独立性测试

测试记录以及最后结果（符合/不符合），开发者应提供能适合第三方测试的产品。

5.5.4.7 脆弱性评定

5.5.4.7.1 脆弱性分析

脆弱性分析应满足如下要求：

a） 开发者提供的脆弱性分析文档应从用户可能破坏安全策略的明显途径出发，对防火墙的各种功能进行分析；

b） 对被确定的脆弱性，评估开发者应明确记录采取的措施；

c） 对每一条脆弱性，应有证据显示在使用防火墙的环境中该脆弱性不能被利用；

d） 所提供的文档应表明经过标识脆弱性的防火墙可以抵御明显的穿透性攻击；

e） 开发者提供的分析文档，应阐明指南性文档是完整的。

6 测评方法

6.1 总体说明

测评方法与技术要求一一对应，它给出具体的测评方法来验证防火墙产品是否达到技术要求中所提出的要求。它由测试环境、测试工具、测试方法和预期结果四个部分构成。

6.2 功能测试

6.2.1 测试环境与工具

功能测试环境示意图可参见图1。其中，路由模式下，172.16.3.x为外部网络地址，192.168.2.x为DMZ网络地址，192.168.1.x为内部网络地址；透明模式下，内部网络、外部网络和DMZ均配置为192.168.1.x网络地址。

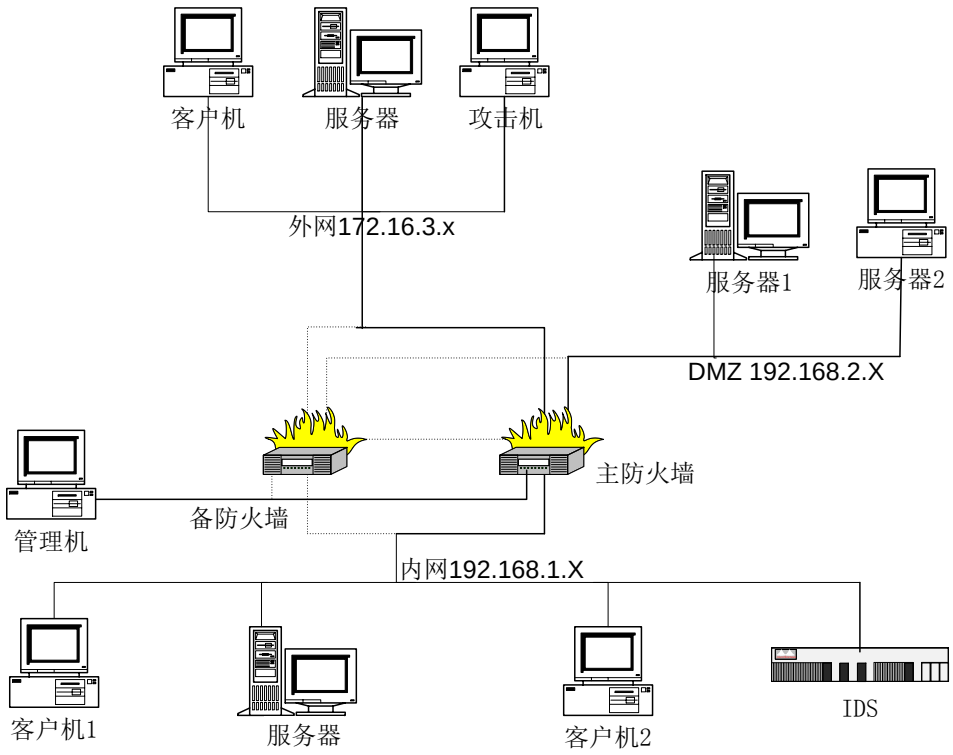


图1 防火墙功能测试环境示意图

功能测试需要的工具有：专用防火墙测试系统或模块，协议分析仪或包捕获工具，以及IP包仿真器。

6.2.2 包过滤

a） 测试方法

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。

b） 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。

6.2.3 状态检测

a）测试方法

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。

b）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。

6.2.4 深度包检测

a）测试方法

1）配置基于URL的内容过滤策略，产生相应的网络会话；

2）配置基于基于电子邮件Subject、To、From域等的内容过滤策略，产生相应的网络会话；

3）配置基于文件类型的内容过滤策略，产生相应的网络会话；

4）配置基于用户的内容过滤策略，产生相应的网络会话；

5）配置基于HTTP和电子邮件关键字的内容过滤策略，产生相应的网络会话。

b）预期结果

1）应能够基于URL进行访问控制；

2）应能够基于电子邮件Subject、To、From域进行访问控制；

3）应能够基于文件类型进行访问控制；

4）应能够基于用户进行访问控制；

5）应能够基于HTTP和电子邮件关键字进行访问控制。

6.2.5 应用代理

a）测试方法

1）分别为内部网络用户访问外部网络、外部网络用户访问DMZ服务器设置代理功能，产生相应的网络会话；

2）通过协议分析仪，检查一个网络会话是否被分为内外两个会话；

3）检查客户端是否需要设置代理服务器地址；

4）为应用代理配置不同的安全策略，检查安全策略的有效性。

b）预期结果

1）防火墙应用代理功能工作正常；

2）网络会话被分割为内外两个会话；

3）如果客户端不需要设置代理服务器，则为透明应用代理；

4）防火墙应能够根据应用层控制域设定安全策略对网络会话进行访问控制。

6.2.6 NAT

a）测试方法

1）为内部网络用户访问外部网络主机分别设置“多对一”和“多对多”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）为外部网络用户访问DMZ服务器分别设置“一对多”和“多对多”DNAT，检查外部网络的主机能否通过防火墙访问DMZ的服务器；

3） 在内部网络、外部网络和DMZ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。

b） 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DMZ的服务器；

3） 实现“多对一”或“多对多”SNAT和DNAT，数据包的源地址和目的地址正确转换。

6.2.7 IP/MAC 地址绑定

a） 7.1.6 .1 测试方法

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。

b） 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。

6.2.8 动态开放端口

a） 测试方法

1） 设置防火墙动态开放端口策略以支持以下应用；

2） 内部网络主机通过FTP（包括主动模式和被动模式）访问外部网络，检查防火墙是否能及时打开FTP数据连接所使用的动态端口，网络会话是否连接正常；

3） 使用支持H.323协议的视频工具（如NetMeeting）在内部网络和外部网络中的用户发起视频会议，检查防火墙是否能及时打开所使用的动态端口，视频会议是否正常进行；

4） 内部网络主机访问外部网络SQL服务器，检查防火墙是否支持SQL*NET数据库协议；

5） 设置内部网络和外部网络的主机在同一VLAN，产生特定的网络会话，检查防火墙是否支持VLAN。

b） 预期结果

1） FTP运行正常， FTP数据连接所使用的动态端口打开；

2） 视频会议正常，H.323协议所使用的动态端口打开；

3） SQL*NET数据库协议的动态端口打开；

4） 防火墙支持VLAN。

6.2.9 策略路由

a） 测试方法

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。

b） 预期结果

1） 支持上述至少一种策略路由策略；

2） 防火墙策略路由工作正常。

6.2.10 流量统计

a） 测试方法

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。

b） 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。

6.2.11 带宽管理

a） 测试方法

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。

b） 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。

6.2.12 双机热备

a） 测试方法

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。

b） 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。

6.2.13 负载均衡

a） 测试方法

1） 设置防火墙负载均衡策略；

2） 在外部网络主机上，产生大量访问DMZ中服务器的网络流量；

3） 通过协议分析仪或包捕获工具观察网络流量，根据数据包源目标地址和流量大小，检查防火墙是否成功地实现了负载均衡功能；

4） 设置防火墙集群工作模式，使多台防火墙集群工作，测试是否达到负载均衡效果。

b） 预期结果

1） 防火墙能够将网络访问均衡到多台服务器上；

2） 防火墙可实现集群工作模式，多台防火墙均衡网络负载。

6.2.14 VPN

a） 测试方法

1） 分别创建防火墙至防火墙、防火墙至客户端的VPN隧道，产生相应的网络会话；

2） 检查VPN隧道的加密算法、认证算法等属性；

3） 通过协议分析仪和协议符合性测试工具，测试VPN会话是否符合协议规范并是安全的。

b） 预期结果

1） 防火墙成功建立VPN隧道，网络会话正常；

2） VPN隧道所使用的加密算法和认证算法符合国家要求；

3） VPN隧道中的通信数据符合协议规范并且是安全的。

6.2.15 协同联动

a） 测试方法

1） 以IDS联动为例，进行测试；

2） 配置防火墙联动策略，并设定认证方式；

3） 外部网络主机向内部网络主机发起策略定义为阻断的攻击，检查防火墙是否能够及时接收IDS报警，并拦截该攻击；

4） 大量发起策略定义为阻断的攻击，测试防火墙是否因联动而造成拒绝服务。

b） 预期结果

1） 防火墙及时响应受信任的并通过认证的IDS的报警信息，并拦截攻击；

2） 防火墙不会因联动而导致拒绝服务。

6.2.16 安全审计

a） 测试方法

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FTP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。

b） 预期结果

1） 防火墙准确记录上述各种事件；

2） 非授权管理员不能访问日志；

3） 授权管理员能进行日志查阅、保存、删除和清空的操作；

4） 能对审计事件进行检索和排序；

5） 日志安全保存；

6） 应只能使用日志管理工具来管理日志，确保日志安全；

7） 存储耗尽时，能够采取技术要求中的操作；

8） 支持统计分析和报表功能。

6.2.17 管理

a） 测试方法

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。

b） 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） 防火墙支持生物特征鉴别；

4） 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；

5） 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；

6） 防火墙支持分权管理，对防火墙的不同管理功能进行分割；

7） 远程管理中管理员和防火墙之间的会话安全；

8） 防火墙的加密符合国家密码管理的有关规定。

6.3 性能测试

6.3.1 测试环境与工具

将专用性能测试仪器与防火墙直接相连，进行测试，如图2所示。性能测试工具主要是专用性能测试设备。

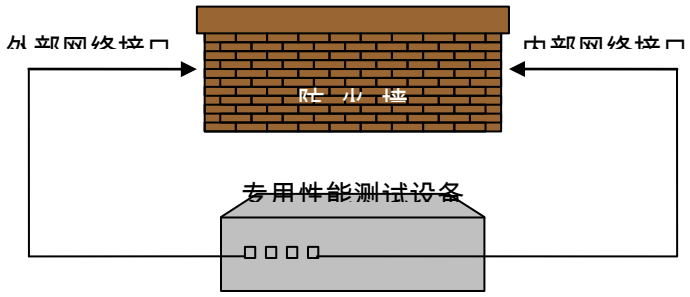


图2 防火墙性能测试环境示意图

6.3.2 吞吐量

a） 测试方法

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。

b） 预期结果

防火墙的吞吐量性能指标应达到通用技术要求5.3.1中规定的最低要求。

6.3.3 延迟

a） 测试方法

1） 配置防火墙只有一条默认允许规则；

2） 取6.3.2中测得的最大吞吐量，进行延迟测试；

3） 配置防火墙有200条以上不同访问控制规则；

4） 取6.3.2中测得的最大吞吐量，进行延迟测试。

b） 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。

6.3.4 最大并发连接数

a） 测试方法

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。

b） 预期结果

防火墙的最大并发连接数性能指标应达到技术要求5.3.3中规定的最低要求。

6.3.5 最大连接速率

a） 测试方法

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。

b） 预期结果

防火墙的最大连接速率性能指标应达到技术要求5.3.4中规定的最低要求。

6.4 安全性测试

6.4.1 测试环境与工具

与功能测试环境相同，如图2所示。测试工具有专用防火墙测试系统、IP包仿真器、渗透测试软件包。

6.4.2 抗渗透

a） 测试方法

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） 采用邮件炸弹攻击工具，对防火墙所保护的电子邮件服务器进行攻击；

6） 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。

b） 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） 防火墙工作正常，不同等级产品防御垃圾邮件的能力不同，应满足5.4.2.2和5.4.3.2中的技术要求；

5） 防火墙性能不应受到明显影响。

6.4.3 恶意代码防御

a） 测试方法

1） 从外部网络给防火墙所保护的Web服务器和电子邮件服务器发送不同的含有恶意代码的数据；

2） 在外部网络通过木马等恶意代码的客户端程序连接内部网络或DMZ上受木马感染的服务器或主机。

b） 预期结果

1） 防火墙工作正常，不同等级的防火墙防御恶意代码攻击的能力不同，应满足5.4.1.3、5.4.2.3和5.4.3.3中的技术要求；

2） 木马行为被阻断，活动的恶意代码行为被检测拦截。

6.4.4 支撑系统

a） 测试方法

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。

b） 预期结果

防火墙支撑系统测试结果应满足5.4.1.4、5.4.2.4和5.4.3.4的技术要求。

6.4.5 非正常关机

a） 测试方法

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。

b） 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。

6.5 保证要求测试

6.5.1 配置管理

a） 测试方法

1） 检查防火墙的版本号，应与所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。

b） 预期结果

防火墙的配置管理测试结果应满足5.5.2.1、5.5.3.1和5.5.4.1的技术要求。

6.5.2 交付与运行

a） 测试方法

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。

b） 预期结果

防火墙的交付和运行测试结果应满足5.5.2.2、5.5.3.2和5.5.4.2的技术要求。

6.5.3 安全功能开发过程

a） 测试方法

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。

b） 预期结果

防火墙的开发保证要求的测试结果应满足5.5.2.3、5.5.3.3和5.5.4.3的技术要求。

6.5.4 指导性文档

a） 测试方法

1） 审查防火墙的管理员指南；

2） 审查防火墙的用户指南。

b） 预期结果

防火墙的指南文件测试结果应满足5.5.2.4、5.5.3.4和5.5.4.4的技术要求。

6.5.5 生命周期支持

a） 测试方法

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。

b） 预期结果

防火墙的测试保证要求的测试结果应满足5.5.2.5和5.5.4.5的技术要求。

6.5.6 测试

a） 测试方法

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。

b） 预期结果

防火墙的测试保证要求的测试结果应满足5.5.2.6、5.5.3.5和5.5.4.6的技术要求。

6.5.7 脆弱性评定

a） 测试方法

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。

b） 预期结果

防火墙的脆弱性分析的测试结果应满足5.5.3.6和5.5.4.7的技术要求。

附录 A

（资料性附录）

防火墙介绍

A.1 概述

防火墙是指设置在不同网络（如可信任的企业内部网络和不可信的公共网络）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据网络安全策略控制（允许、拒绝、监测）出入网络的信息流，且自身具有较强的抗攻击能力。它是提供信息安全服务，实现网络与信息安全的基础设施。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了流经防火墙的数据，保证了内部网络和DMZ的安全。

防火墙通常分为包过滤、应用代理和包过滤与应用代理相结合的复合型三种类型。包过滤型防火墙允许内外部网络络的直接连接，依据IP地址、协议等关键字进行访问控制。应用代理型防火墙不允许内外部网络络的直接连接，将连接分为两个部分，代理内外部网络络的连接请求与应答，安全性更高。复合型防火墙是两者的结合。

防火墙可以是软件、硬件或软硬件的组合。其中，软件形式的防火墙较少，具有安装灵活，便于升级扩展等优点，缺点是安全性受制于其支撑操作系统平台，性能不高；纯硬件防火墙基于ASIC（Application Specific Integrated Circuit，特定用途集成电路）开发，性能优越，但可扩展性、灵活性较差；软硬结合的防火墙大多基于网络处理器（Network Processor，简称NP）开发，性能较高，也具备一定的可扩展性和灵活性。

A.2 工作模式

防火墙通常以路由模式或透明模式运行。

A.2.1 路由模式

在路由模式下，防火墙相当于一个路由器，有外部网络、内部网络和DMZ网络接口IP地址。

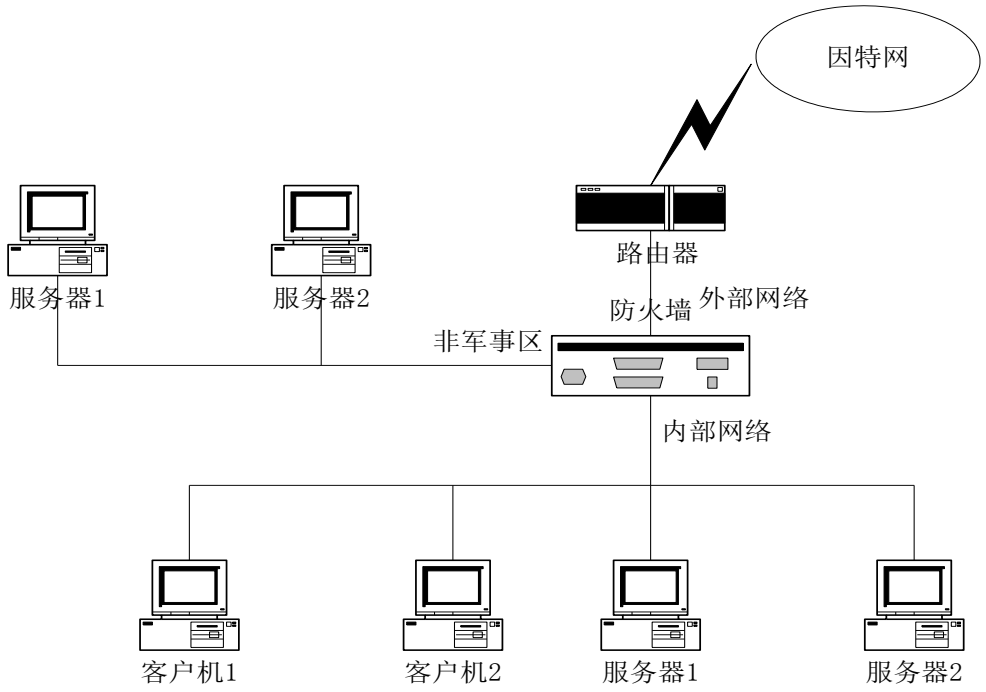
A.2.2 透明模式

透明模式也称桥模式，防火墙以网桥的形式接入网络，而不需要改变网络的拓扑结构。用户将不必重新设定和修改路由，也不需要知道防火墙的位置，防火墙就可以直接安装和放置到网络中使用。

A.3 工作环境

防火墙通常将网络划分为若干个区域，通过定义区域之间的访问控制策略来保护内部网络和DMZ的安全，抵御来自外部网络的各种非法网络攻击。

图A.1是一个典型的防火墙应用环境。它将网络分为内部网络、外部网络和DMZ三个区域。内部网络是一个可信区域，外部网络是一个不可信区域，DMZ中的服务器可以向外部网络和内部网络用户提供应用服务。



图A.1 防火墙应用环境示意图