湖北省医疗器械质量监督检验研究院

网络安全验证培训

信息技术研究中心 胡艺
18907292266
huyi@whmit.cn

医疗器械网络安全的概念

一、适用范围

本指导原则适用于医疗器械网络安全的注册申报，包括具备电子数据交换、远程访问与控制、用户访问三种功能当中一种及以上功能的第二、三类独立软件和含有软件组件的医疗器械（包括体外诊断医疗器械）；适用于自研软件、现成软件的注册申报。

其中，网络包括无线、有线网络，电子数据交换包括基于网络、存储媒介的单向、双向数据传输，远程访问与控制包括基于网络的实时、非实时的访问与控制，用户（如医务人员、患者、维护人员等）访问包括基于软件用户界面、电子接口的人机交互方式。

本指导原则也可用作医疗器械软件、质量管理软件的体系核查参考。

此外，尽管信息安全、网络安全、数据安全的定义和范围各有侧重，既有联系又有区别，不尽相同，但本指导原则从医疗器械安全有效性评价角度出发对三者不做严格区分，统一采用网络安全进行表述，即从网络安全角度综合考虑医疗器械的信息安全和数据安全。

医疗器械网络安全的概念

（二）医疗器械相关数据

医疗器械相关数据可分为医疗数据和设备数据。

医疗数据是指医疗器械所产生的、使用的与医疗活动相关的数据（含日志），从个人信息保护角度又可分为敏感医疗数据、非敏感医疗数据，其中敏感医疗数据是指含有个人信息的医疗数据[3]，反之即为非敏感医疗数据。个人信息是指以电子或者其他方式记录的能够单独或与其他信息结合识别自然人个人身份的各种信息，如自然人的姓名、出生日期、身份证件号码、个人生物识别信息（含容貌信息）、住址、电话号码等。

设备数据是指记录医疗器械运行状况的数据（含日志），用于监视、控制医疗器械运行或者医疗器械的维护与升级，不得含有个人信息。

注册申请人需基于医疗器械相关数据的类型、功能、用途，结合网络安全特性考虑医疗器械网络安全要求。同时，保证敏感医疗数据所含个人信息免于泄露、滥用和篡改，以及医疗数据和设备数据的有效隔离（如访问权限控制等方法）。

信息安全技术　个人信息安全规范

1　范围

本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动的原则和安全要求。

本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

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 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的判定方法和类型参见附录 A。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

3.2

个人敏感信息　personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：关于个人敏感信息的判定方法和类型参见附录 B。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

医疗器械网络安全的概念

表 A.1　个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据(通常称为元数据)等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码(如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等)等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

表 B.1　个人敏感信息举例

个人财产信息	银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

医疗器械网络安全的概念

6 个人信息的存储

6.1 个人信息存储时间最小化

对个人信息控制者的要求包括：

a) 个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外；

b) 超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

6.2 去标识化处理

收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

6.3 个人敏感信息的传输和存储

对个人信息控制者的要求包括：

a) 传输和存储个人敏感信息时，应采用加密等安全措施；

注 1：采用密码技术时宜遵循密码管理相关国家标准。

b) 个人生物识别信息应与个人身份信息分开存储；

c) 原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：

1) 仅存储个人生物识别信息的摘要信息；

2) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

3) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

注 2：摘要信息通常具有不可逆特点，无法回溯到原始信息。

注 3：个人信息控制者履行法律法规规定的义务相关的情形除外。

6.4 个人信息控制者停止运营

当个人信息控制者停止运营其产品或服务时，应：

a) 及时停止继续收集个人信息；

b) 将停止运营的通知以逐一送达或公告的形式通知个人信息主体；

c) 对其所持有的个人信息进行删除或匿名化处理。

网络安全能力

本指导原则所述医疗器械网络安全能力包括：

1.自动注销（ALOF）：产品在无人值守期间阻止非授权用户访问和使用的能力。

2.审核（AUDT）：产品提供用户活动可被审核的能力。

3.授权（AUTH）：产品确定用户已获授权的能力。

4.节点鉴别（NAUT）：产品鉴别网络节点的能力。

5.人员鉴别（PAUT）：产品鉴别授权用户的能力。

6.连通性（CONN）：产品保证连通网络安全可控的能力。

7.物理防护（PLOK）：产品提供防止非授权用户访问和使用的物理防护措施的能力。

8.系统加固（SAHD）：产品通过固化措施对网络攻击和恶意软件的抵御能力。

9.数据去标识化与匿名化（DIDT）：产品直接去除、匿名化数据所含个人信息的能力。

10.数据完整性与真实性（IGAU）：产品确保数据未以非授权方式更改且来自创建者或提供者的能力。

11.数据备份与灾难恢复（DTBK）：产品的数据、硬件或软件受到损坏或破坏后恢复的能力。

12.数据存储保密性与完整性（STCF）：产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。

13.数据传输保密性（TXCF）：产品确保数据传输保密性的能力。

14.数据传输完整性（TXIG）：产品确保数据传输完整性的能力。

15.网络安全补丁升级（CSUP）：授权用户安装/升级产品网络安全补丁的能力。

16.现成软件清单（SBOM）：产品为用户提供全部现成软件清单的能力。

17.现成软件维护（RDMP）：产品在全生命周期中对现成软件提供网络安全维护的能力。

18.网络安全使用指导（SGUD）：产品为用户提供网络安全使用指导的能力。

19.网络安全特征配置（CNFS）：产品根据用户需求配置网络安全特征的能力。

20.紧急访问（EMRG）：产品在预期紧急情况下允许用户访问和使用的能力。

21.远程访问与控制（RMOT）：产品确保用户远程访问与控制（含远程维护与升级）的网络安全的能力。

22.恶意软件探测与防护（MLDP）：产品有效探测、阻止恶意软件的能力。

网络安全能力

本指导原则所述医疗器械网络安全能力包括：

1.自动注销（ALOF）：产品在无人值守期间阻止非授权用户访问和使用的能力。

2.审核（AUDT）：产品提供用户活动可被审核的能力。

3.授权（AUTH）：产品确定用户已获授权的能力。

4.节点鉴别（NAUT）：产品鉴别网络节点的能力。

5.人员鉴别（PAUT）：产品鉴别授权用户的能力。

6.连通性（CONN）：产品保证连通网络安全可控的能力。

7.物理防护（PLOK）：产品提供防止非授权用户访问和使用的物理防护措施的能力。

8.系统加固（SAHD）：产品通过固化措施对网络攻击和恶意软件的抵御能力。

9.数据去标识化与匿名化（DIDT）：产品直接去除、匿名化数据所含个人信息的能力。

10.数据完整性与真实性（IGAU）：产品确保数据未以非授权方式更改且来自创建者或提供者的能力。

11.数据备份与灾难恢复（DTBK）：产品的数据、硬件或软件受到损坏或破坏后恢复的能力。

12.数据存储保密性与完整性（STCF）：产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。

13.数据传输保密性（TXCF）：产品确保数据传输保密性的能力。

14.数据传输完整性（TXIG）：产品确保数据传输完整性的能力。

15.网络安全补丁升级（CSUP）：授权用户安装/升级产品网络安全补丁的能力。

16.现成软件清单（SBOM）：产品为用户提供全部现成软件清单的能力。

17.现成软件维护（RDMP）：产品在全生命周期中对现成软件提供网络安全维护的能力。

18.网络安全使用指导（SGUD）：产品为用户提供网络安全使用指导的能力。

19.网络安全特征配置（CNFS）：产品根据用户需求配置网络安全特征的能力。

20.紧急访问（EMRG）：产品在预期紧急情况下允许用户访问和使用的能力。

21.远程访问与控制（RMOT）：产品确保用户远程访问与控制（含远程维护与升级）的网络安全的能力。

22.恶意软件探测与防护（MLDP）：产品有效探测、阻止恶意软件的能力。

网络安全送检资料

- 网络安全验证方案（必须，检验依据）
- 最小单元标签样稿（必须，软件标识/铭牌）
- 说明书（可选）
- 自测资料（可选，内部测试记录）

网络安全验证方案

1 简介

1.1 目的

该验证方案用于...软件网络安全的验证，本文适用于该项目开发人员和测试人员。

1.2 背景

针对...软件网络安全需求，进行测试计划编写。

1.3 参考文档

《医疗器械网络安全注册审查指导原则（2022 年修订版）》
《医疗器械软件注册审查指导原则（2022 年修订版）》
《人工智能医疗器械注册审查指导原则》
《...技术要求》

2 测试资源要求

网络安全测试资源以实际为准。

软件正常运行所需的典型运行环境见下表：

...

3 测试项目

3.1 漏洞评估

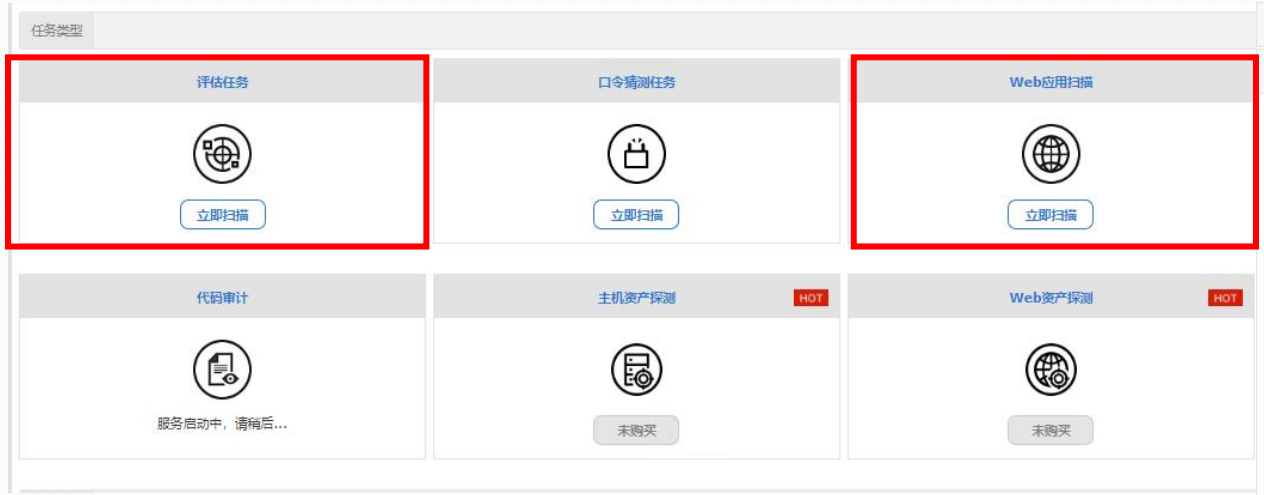
3.1.1 静态检测

使用卡巴斯基杀毒软件扫描软件安装文件以及相关文件。

3.1.2 漏洞扫描

使用漏洞扫描软件工具(绿盟 RSAS)的 WEB 应用扫描功能，对...软件进行漏洞扫描。按照 CVSS 漏洞等级对...软件扫描出的已知漏洞总数和已知剩余漏洞数进行评估。

绿盟RSAS


任务类型
评估任务
立即扫描
口令猜测任务
立即扫描
Web应用扫描
立即扫描
代码审计
服务启动中，请稍后...
主机资产探测
HOT
未购买
Web资产探测
HOT
未购买


NSFOCUS
绿盟科技"远程安全评估系统"安全评估报告
目录
1.综述信息
1.1任务信息
网络风险
比较危险（5.1分）
任务名称
扫描任务
扫描目标
任务类型
WEB应用扫描
任务状态
扫描完成
漏洞扫描模板
自动匹配扫描
下达任务用户
admin
任务数据来源
本地扫描
任务说明
信息统计
已爬取文件数：47
有漏洞文件数：10
已扫描链接数：54
已爬取链接数：78
域名统计
已扫描域名数：1
非常危险域名数：0
时间统计
开始：2023-09-15 13:30:44
结束：2023-09-15 13:40:45
历时：10分1秒
版本信息
系统版本：V6.0R04F03SP02
Web插件版本：V6.0R02F00.3108
1.2风险分布
1.2.1页面风险级别分布
页面风险级别分布
2.1%
19.1%
78.7%
高风险[0个]
中风险[1个]
低风险[9个]
无风险[37个]
合计 17个页面

绿盟RSAS

3.漏洞列表

3.1漏洞分布

漏洞类别：中危险[1] 低风险[11]

序号	漏洞名称	影响页面个数	出现次数
1	检测到目标站点存在javascript框架库漏洞	1	1
2	检测到目标服务器存在应用程序错误	1	1
3	jQuery 存在 XSS 漏洞	1	1
4	检测到会话cookie中缺少HttpOnly属性	1	1
5	检测到目标站点可能存在跨站请求伪造漏洞	6	7
6	检测到目标X-XSS-Protection响应头缺失	1	1
7	检测到目标Content-Security-Policy响应头缺失	1	1
8	检测到目标URL存在电子邮件地址模式	1	1
9	检测到目标X-Permitted-Cross-Domain-Policies响应头缺失	1	1
10	检测到目标X-Download-Options响应头缺失	1	1
11	检测到目标Strict-Transport-Security响应头缺失	1	1
12	检测到目标网站存在上传下载相关的目录和文件	1	1
合计		17	18

序号	漏洞名称	影响页面个数	出现次数
1	检测到目标站点存在javascript框架库漏洞	1	1

受影响站点	
详细描述	JavaScript 框架或库是一组能轻松生成跨浏览器兼容的 JavaScript 代码的工具和函数。如果网站使用了存在漏洞的 JavaScript 框架或库，攻击者就可以利用此漏洞来劫持用户浏览器，进行挂马、XSS、Cookie劫持等攻击。
解决办法	将受影响的javascript框架库升级到最新版本。
威胁分值	6
危险插件	否
发现日期	2001-01-01
CVSS评分	6.1(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

nessus

Scan Information

Start time: Sat Sep 16 12:48:46 2023

End time: Sat Sep 16 13:04:17 2023

Host Information

IP:

OS: Microsoft Windows 10

nessus

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/3389

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX          Auth     Encryption             MAC
   ----------------------        ----------       ---          ----     ---------------------  ---
   DES-CBC3-SHA                  0x00, 0x0A       RSA          RSA      3DES-CBC(168)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

APPSCAN

问题类型 7

TOC

	问题类型	问题的数量
高	已解密的登录请求	1
中	"Content-Security-Policy"头缺失	1
中	"X-Content-Type-Options"头缺失或不安全	1
中	在应用程序中发现不必要的 Http 响应头	1
中	查询中接受的主体参数	1
参	"Referral Policy" Security 头缺失	1
参	发现电子邮件地址模式	1

有漏洞的 URL 4

TOC

	URL	问题的数量
高	http://[redacted]23/login	2
中	http://[redacted]3/	3
中	http://[redacted]/static/md5.js	1
参	http://[redacted]tatic/jsencrypt.js	1

APPSCAN

修订建议 7

TOC

	修复任务	问题的数量
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	1
中	将服务器配置为使用值为"nosniff"的"X-Content-Type-Options"头	1
中	将服务器配置为使用安全策略的"Content-Security-Policy"头	1
中	请勿允许敏感信息泄漏。	1
中	请勿接受在查询字符串中发送的主体参数	1
低	将服务器配置为使用安全策略的 "Referrer Policy" 头	1
低	除去 Web 站点中的电子邮件地址	1

APPSCAN

已解密的登录请求

严重性：	高
CVSS 分数：	8.2
URL：	http://[redacted]/login
实体：	password (Parameter)
风险：	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因：	SSL（安全套接字层）可为 HTTP 提供数据机密性和完整性。通过加密 HTTP 消息，SSL 可防止攻击者窃听或更改消息内容。登录页应始终采用 SSL 来保护从客户机传输到服务器的用户名和密码。如果不使用 SSL，会使用户凭证在传输到服务器期间作为明文公开，从而易被窃听。
固定值：	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异：

推理： AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应：

```
POST /login HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer:
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 32

username=&password=&vercode=1234

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Vary: Cookie
Server: Microsoft-IIS/10.0
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
```

网络安全验证方案

3.2 网络安全能力测试

序号	网络安全能力	网络安全能力描述	测试用例名称	测试步骤	预期结果
1.	ALOF 自动注销	产品在无人值守期间阻止非授权用户访问和使用的能力。			
2.	AUDT 审核	产品提供用户活动可被审核的能力。			
3.	AUTH 授权	产品确定用户已获授权的能力。			
4.	NAUT 节点鉴别	产品鉴别网络节点的能力。			

……

医疗器械网络安全注册审查指导原则（22条）

1. 自动注销（ALOF）：产品在无人值守期间阻止非授权用户访问和使用的能力。
2. 审核（AUDT）：产品提供用户活动可被审核的能力。
3. 授权（AUTH）：产品确定用户已获授权的能力。
4. 节点鉴别（NAUT）：产品鉴别网络节点的能力。
5. 人员鉴别（PAUT）：产品鉴别授权用户的能力。
6. 连通性（CONN）：产品保证连通网络安全可控的能力。
7. 物理防护（PLOK）：产品提供防止非授权用户访问和使用的物理防护措施的能力。

审核（AUDT）

通过审核追踪对系统的数据访问、修改或删除予以记录，从而跟踪和检查系统的活动。

审核日志应记录了以下事件:登录/注销、创建/修改/删除、从可移动介质中导入/导出、外部系统（网络）接收/传输数据、远程服务活动等。还包括审核日志中记录的单个事件识别信息:使用者ID/操作时间等等。

授权（AUTH）

避免未经授权访问数据和功能，以确保系统和数据的保密性、完整性和可用性，以及确保数据和系统的有限制使用。

包括医疗器械是否可以通过用户登录要求或其他机制防止未经授权用户访问；是否可以根据“角色”（例如:访客、普通用户，高级用户、管理员等）在应用程序中为用户赋予不同的特权级；以及器械所有者/操作员是否可以获得不受限制的管理特权。

医疗器械网络安全注册审查指导原则（22条）

数据去标识化与匿名化（DIDT）

在给定的脱敏规则和策略的情况下，对敏感数据比如手机号、银行卡号等信息，进行转换或者修改，防止敏感数据直接在不可靠的环境下使用。

体现产品识别敏感数据、去标识化、匿名化数据所含个人信息的能力。包括不同使用场景、不同风险等级下的敏感医疗数据分类、个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的能力；个人信息经过处理无法识别特定自然人且不能复原的能力。

8. 系统加固（SAHD）：产品通过固化措施对网络攻击和恶意软件的抵御能力。
9. 数据去标识化与匿名化（DIDT）：产品直接去除、匿名化数据所含个人信息的能力。
10. 数据完整性与真实性（IGAU）：产品确保数据未以非授权方式更改且来自创建者或提供者的能力。
11. 数据备份与灾难恢复（DTBK）：产品的数据、硬件或软件受到损坏或破坏后恢复的能力。
12. 数据存储保密性与完整性（STCF）：产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。

数据存储保密性与完整性（STCF）

保障用户进行数据存储时的数据不被篡改和泄露，并在数据受到篡改和泄露时受到提醒。

包括用户进行数据存储时系统对数据完整性的检测与恢复：应在数据操作时进行完整性检测、以发现数据完整性被破坏的情况；并在检测到完整性错误时，采取必要的恢复措施的能力。

医疗器械网络安全注册审查指导原则（22条）

数据传输保密性（TXCF）

数据在不同介质（内部系统、局域网、互联网）中进行传输时，根据不同的保密要求，确保数据在传输过程中不被泄漏和窃取。

包括用户之间传输的用户数据，根据不同数据类型的不同保密性要求，进行不同程度的保密性保护，确保数据在传输过程中不被泄漏和窃取的能力。

看协议、抓包等方式验证

13. 数据传输保密性（TXCF）：产品确保数据传输保密性的能力。
14. 数据传输完整性（TXIG）：产品确保数据传输完整性的能力。
15. 网络安全补丁升级（CSUP）：授权用户安装/升级产品网络安全补丁的能力。
16. 现成软件清单（SBOM）：产品为用户提供全部现成软件清单的能力。
17. 现成软件维护（RDMP）：产品在全生命周期中对现成软件提供网络安全维护的能力。
18. 网络安全使用指导（SGUD）：产品为用户提供网络安全使用指导的能力。
19. 网络安全特征配置（CNFS）：产品根据用户需求配置网络安全特征的能力。
20. 紧急访问（EMRG）：产品在预期紧急情况下允许用户访问和使用的能力。
21. 远程访问与控制（RMOT）：产品确保用户远程访问与控制（含远程维护与升级）的网络安全的能力。
22. 恶意软件探测与防护（MLDP）：产品有效探测、阻止恶意软件的能力。

数据传输完整性（TXIG）

数据在不同介质（内部系统、局域网、互联网）中进行传输时，能防止用户数据被篡改、删除、插入等情况发生，并在发生时采取恢复措施。

包括经网络传输的用户数据对完整性的检测与恢复：应在数据传输过程中进行完整性检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入等情况发生，并在检测到完整性错误时，采取必要的恢复措施的能力。

看协议、传输前后校验码或摘要比对，如比对MD5码

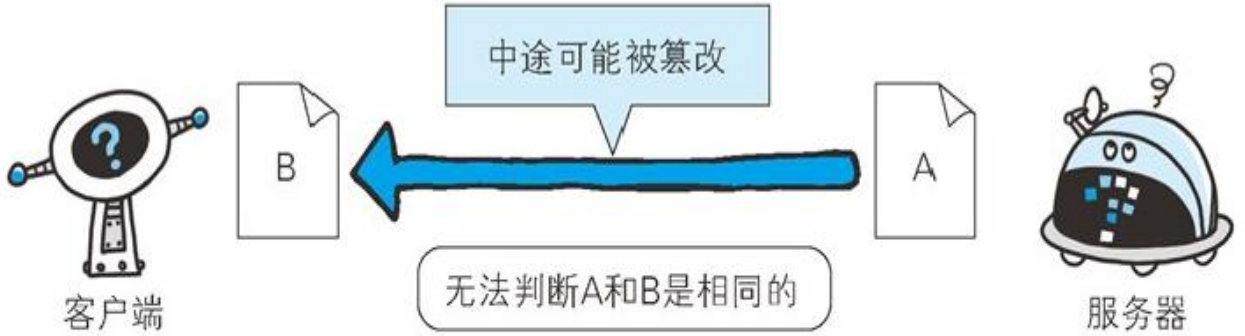
网络安全验证方案-数据传输保密性

7.1 HTTP 的缺点

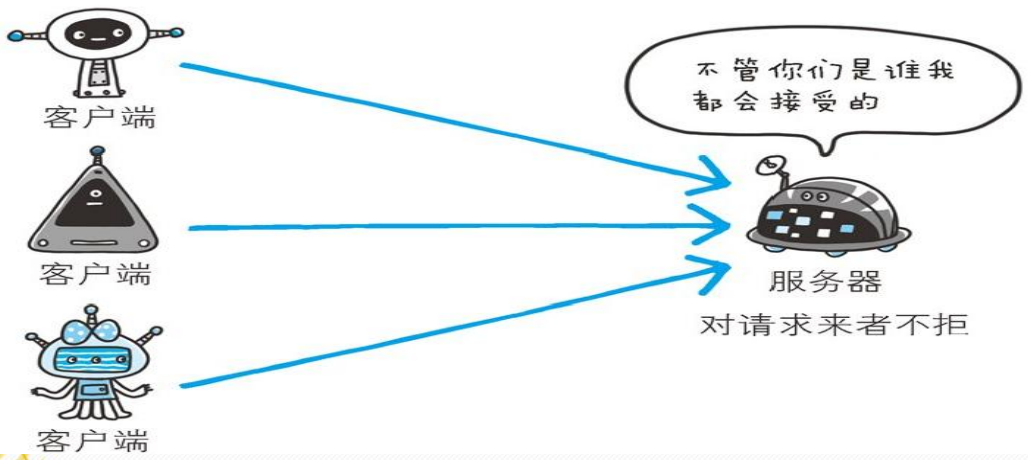
到现在为止，我们已了解到 HTTP 具有相当优秀和方便的一面，然而 HTTP 并非只有好的一面，事物皆具两面性，它也是有不足之处的。

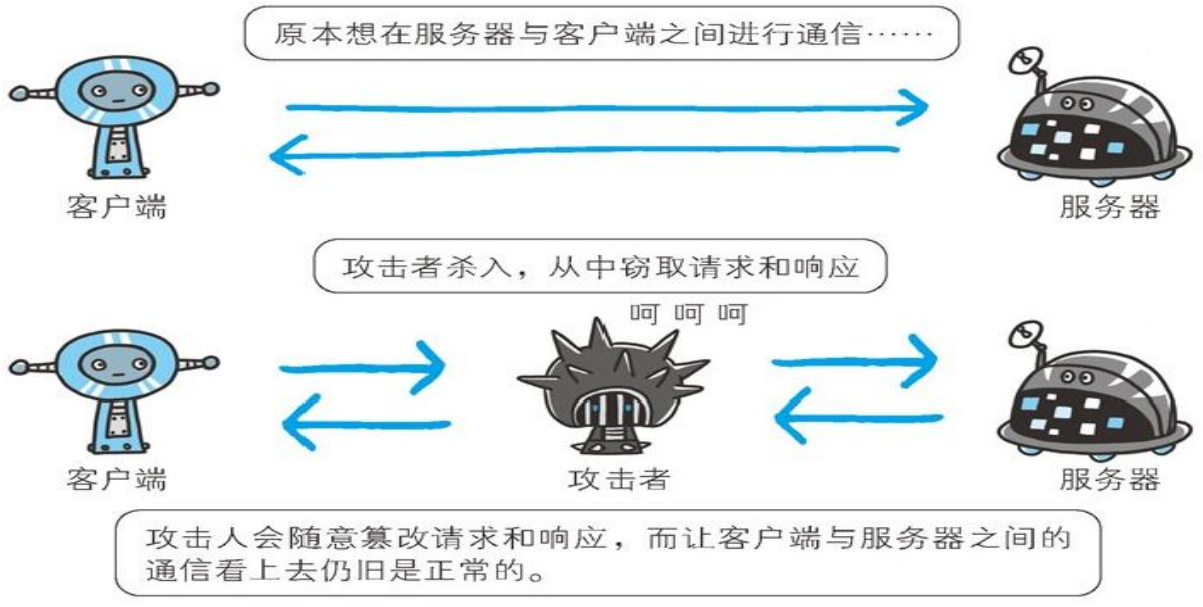
HTTP 主要有这些不足，例举如下。

- 通信使用明文（不加密），内容可能会被窃听
- 不验证通信方的身份，因此有可能遭遇伪装
- 无法证明报文的完整性，所以有可能已遭篡改



比如，从某个 Web 网站上下载内容，是无法确定客户端下载的文件和服务器上存放的文件是否前后一致的。文件内容在传输途中可能已经被篡改为其他的内容。即使内容真的已改变，作为接收方的客户端也是觉察不到的。





网络安全验证方案–数据传输保密性

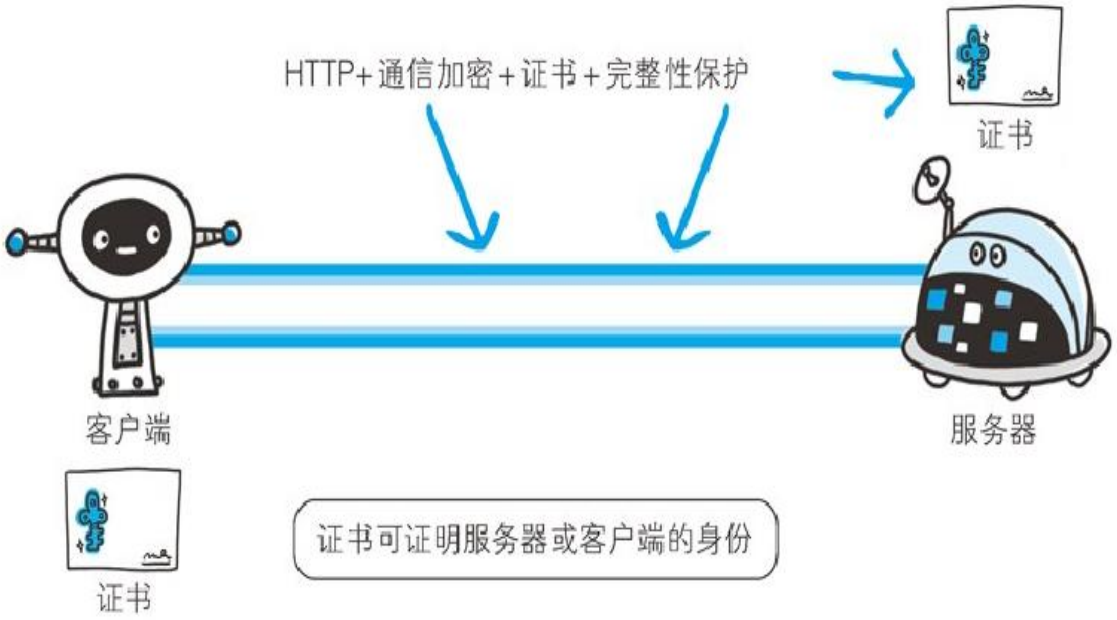
7.2 HTTP+ 加密 + 认证 + 完整性保护 =HTTPS

7.2.1 HTTP 加上加密处理和认证以及完整性保护后即是 HTTPS

如果在 HTTP 协议通信过程中使用未经加密的明文，比如在 Web 页面中输入信用卡号，如果这条通信线路遭到窃听，那么信用卡号就暴露了。

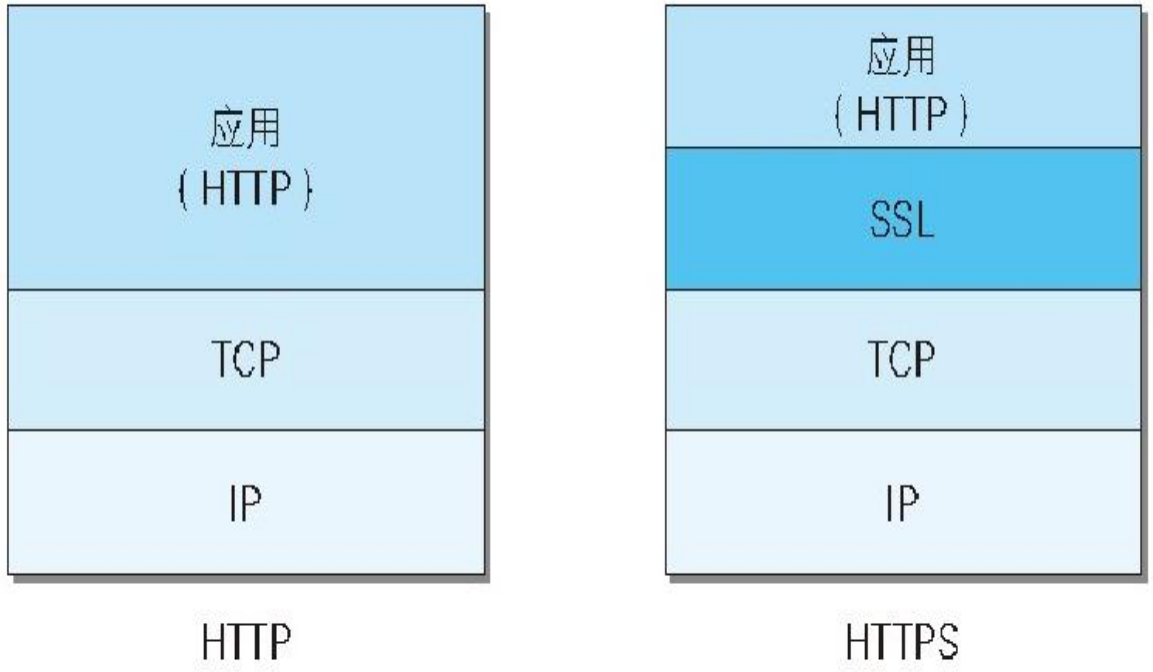
另外，对于 HTTP 来说，服务器也好，客户端也好，都是没有办法确认通信方的。因为很有可能并不是和原本预想的通信方在实际通信。并且还需要考虑到接收到的报文在通信途中已经遭到篡改这一可能性。

为了统一解决上述这些问题，需要在 HTTP 上再加入加密处理和认证等机制。我们把添加了加密及认证机制的 HTTP 称为 HTTPS（HTTP Secure）。



图：使用 HTTPS 通信

通常，HTTP 直接和 TCP 通信。当使用 SSL 时，则演变成先和 SSL 通信，再由 SSL 和 TCP 通信了。简言之，所谓 HTTPS，其实就是身披 SSL 协议这层外壳的 HTTP。



在采用 SSL 后，HTTP 就拥有了 HTTPS 的加密、证书和完整性保护这些功能。

SSL 是独立于 HTTP 的协议，所以不光是 HTTP 协议，其他运行在应用层的 SMTP 和 Telnet 等协议均可配合 SSL 协议使用。可以说 SSL 是当今世界上应用最为广泛的网络安全技术。

网络安全验证方案-数据传输保密性

WebSocket (WS)是HTML5一种新的协议。它实现了浏览器与服务器全双工通信，能更好地节省服务器资源和带宽并达到实时通讯。WebSocket建立在TCP之上，同HTTP一样通过TCP来传输数据，但是它和HTTP最大不同是：

WebSocket是一种双向通信协议，在建立连接后，WebSocket服务器和Browser/Client Agent都能主动的向对方发送或接收数据，就像Socket一样；WebSocket需要类似TCP的客户端和服务器端通过握手连接，连接成功后才能相互通信。

WSS（Web Socket Secure）是WebSocket的加密版本。

.....

```
var ws = new WebSocket("ws://echo.websocket.org");
```

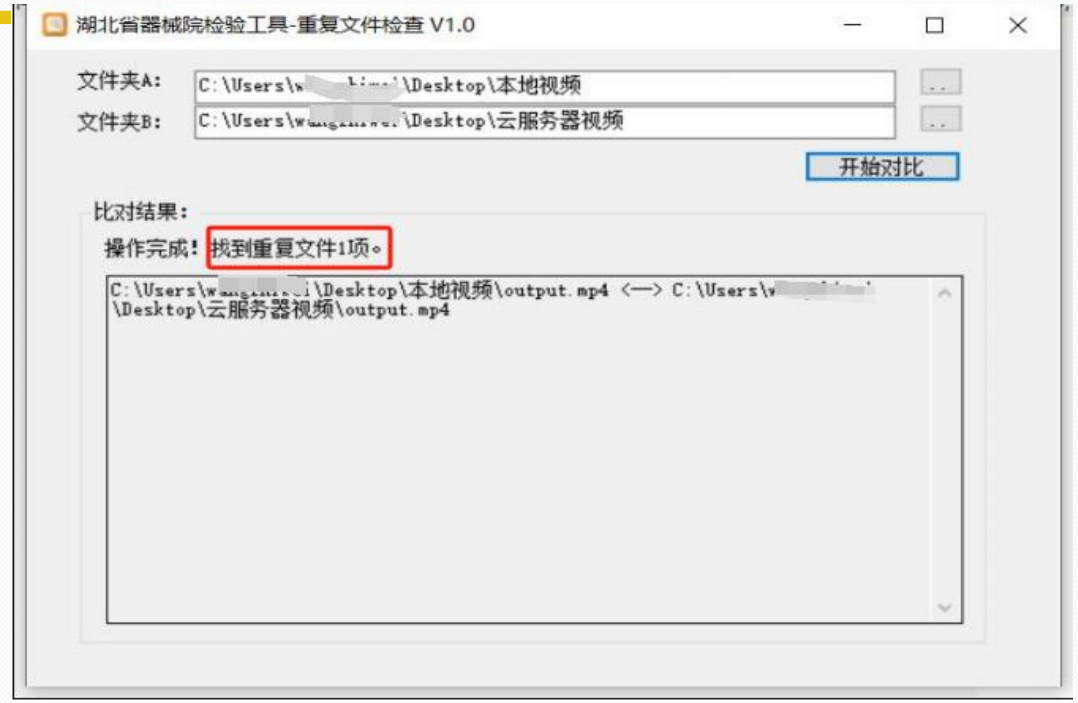
这一行JS代码是在申请一个WebSocket对象，参数是需要连接的服务器端的地址，同http协议使用http://开头一样，WebSocket协议的URL使用ws://开头，另外安全的WebSocket协议使用wss://开头

网络安全验证方案-数据存储保密性与完整性

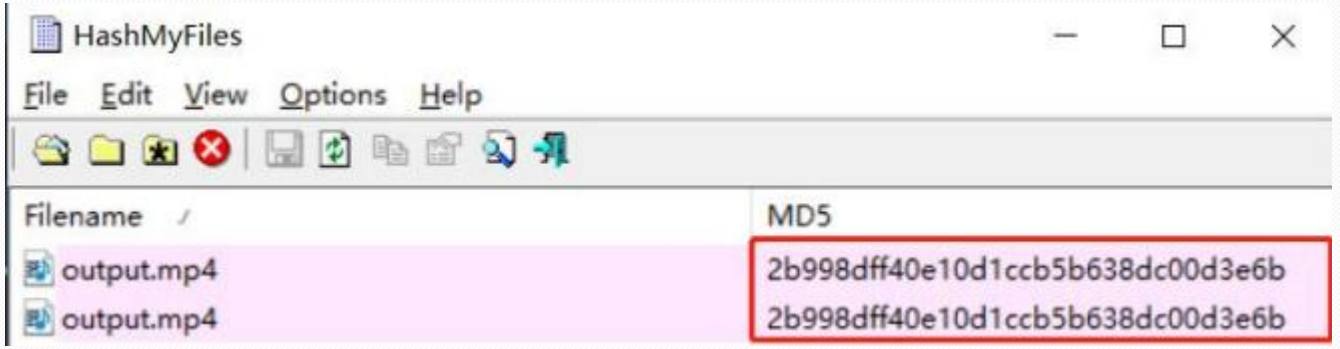
数据库中密码加密

email	password
4[redacted]@qq.com	$2a$10$v04BC9YzAbAcJ.b43UiSueMD8LFgD3GUrAK5GfBC8AXS
	$2a$10$IoBhIMqSuK9C6pd3g/U7XeYhZ79k45JjfmxlKueatYRFdC
k[redacted]o	$2a$10$80s0D5XvQvJRrec5j5AzJOm7fP.zG443PG/Au6C2NOlP9u
	$2a$10$yL6eM3yCpm5xmTV1jnBJu.duT9lfu7P4WO5ffNjBl.a6hFz
	$2a$10$8sAgC7k3oqJFk5JhUBNn5.U5A8CTJE3sXcWXwznnYDs1l
4[redacted]2@qq.com	$2a$10$TYwqK4fQsWlr5eCy7xBPROs2nM.Qxu7eW2KX4sgmNq
	$2a$10$2LEdT.CAYjvvLDifRR2iY.zE1yo5Zms9.F8wV52LjY0.Keo3h
	$2a$10$b6OyFCwo0YSaout38RBCK.uZNM.vuCgi5xq6L3M5RaAr
	$2a$10$k1fvosD2ZZ01GojW6SBm5ORE3Y5QMc3zoLbiTExOrBbC
	$2a$10$Bt2KYM1O8ZMWu.R3w55k/eOlFsimzT/24qt52ecY6Yc1
	$2a$10$dvT0KGKL2WO/MMfs63zV1exMqsI75QWz87YXbbF3Xn

.....



数据完整性对比验证



网络安全验证方案-恶意软件探测与防护

05.01 防火墙是怎样的网络硬件

20 世纪 90 年代，随着互联网的普及，出现了路由器访问控制列表无法抵御的攻击和非法访问等一系列威胁，因此出现了针对这些威胁的防范策略需求。1992 年 OECD 组织发布了“信息系统安全指导书”，其中定义了为构建安全网络体系而需要遵循的 CIA 基本理念。CIA 是机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）三个英文单词的首字母组合，这三个方面的主要威胁及其对策如表 5-1 所示。

表 5-1 CIA 的内容

CIA 条目	威胁的种类	对策使用的技术	对策实施的装置	说明
机密性	窃听、非法访问、窃取等	用户认证、加密	防火墙、VPN、IDS/IPS等	信息的机密性是指只允许合法用户访问相关信息。确保信息的机密性即保证信息不被泄露，设立防止非法访问等保护对策
完整性	篡改、冒充等	数据认证、电子签名、加密	防火墙、VPN、IDS/IPS等	处理正确信息，保证信息的完整和确切，防止信息被篡改
可用性	DoS攻击等	过滤、冗余、策略	防火墙、带宽控制装置等	确保合法用户能够访问授权的信息。需要重视服务器或网络硬件的运维，避免系统出现当机问题

防火墙硬件作为防范装置能够同时实现 CIA 中 3 个条目的相应对策。在 20 世纪 90 年代中期，普通企业一般都会在网关（LAN 与互联网的边界）中设置防火墙。

防火墙（Firewall）是指为了防止发生火灾时，火势蔓延至建筑物内其他区域而设置的、由防火材质（主要是石膏板）铸成的墙（图 5-1）。

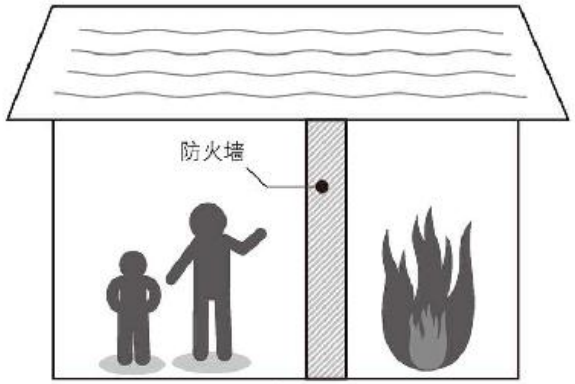


图 5-1 防火墙示意图

将自外而内的网络入侵行为看作火灾，那么防止这种入侵的对策即可称为防火墙。在网络结构图中经常也使用“砖墙”的图标来表示防火墙（图 5-2）。

图 5-2 Windows 中防火墙的图标

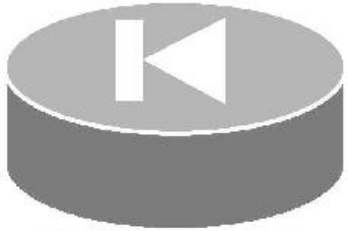


图 5-3 思科公司的防火墙图标

防火墙这个装置原本用于防范外部网络，也就是拥有多个不特定用户的公共网络对内部网络（企业的 Intranet）进行的 DoS 攻击或不法访问（Hacking，黑客行为），但现在也开始需要防范从内部网络向互联网泄露信息或将内部网络作为攻击跳板等行为。

谢谢