网络安全及常见隐患

网络基础

目录

Contents

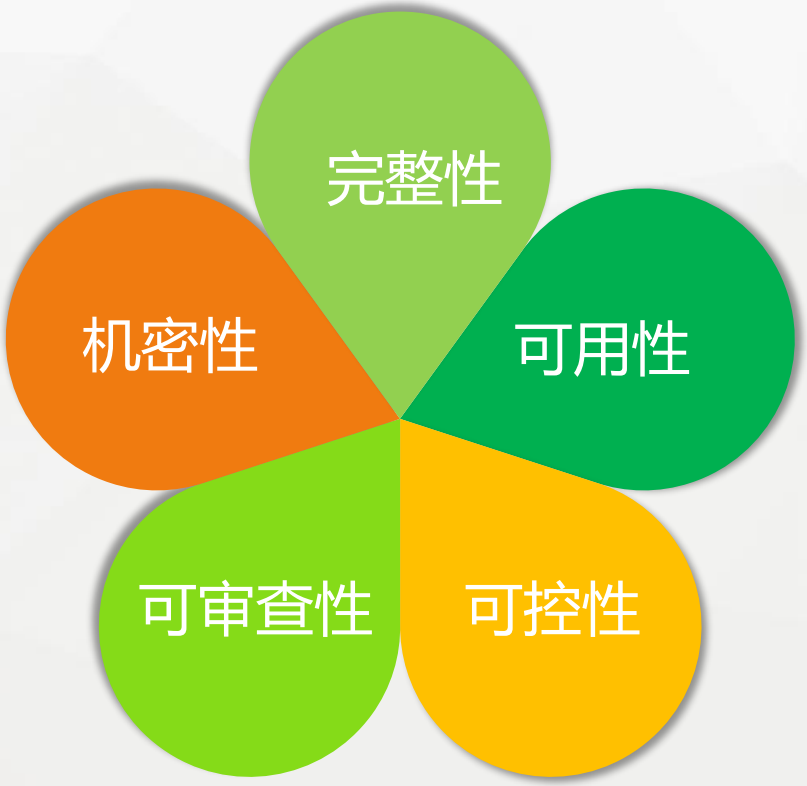
学习目标

- 了解网络安全的概念
- 熟悉网络安全隐患的表现
- 了解网络攻击的两种方式

网络安全

网络安全是指通过采取各种技术与管理措施，使网络系统的硬件、软件及其系统中的数据资源受到保护，不因一些不利因素影响而使这些资源遭到破坏、更改、泄露，保证网络系统连续、可靠、正常的运行。

网络安全五个基本要素:



网络安全隐患

网络安全的隐患是指计算机或其他通信设备利用网络进行交互时可能会受到的窃听、攻击或破坏，它是指具有侵犯系统安全或危害系统资源的潜在的环境、条件或事件。

网络安全隐患表现为:

操作系统脆弱性

数据库系统的脆弱性

网络安全隐患

网络安全的隐患是指计算机或其他通信设备利用网络进行交互时可能会受到的窃听、攻击或破坏，它是指具有侵犯系统安全或危害系统资源的潜在的环境、条件或事件。

网络安全隐患表现为:

数据链路层：Mac欺骗、Mac泛洪、ARP欺骗、STP重定向

网络层：IP欺骗、报文分片、ICMP攻击及路由攻击

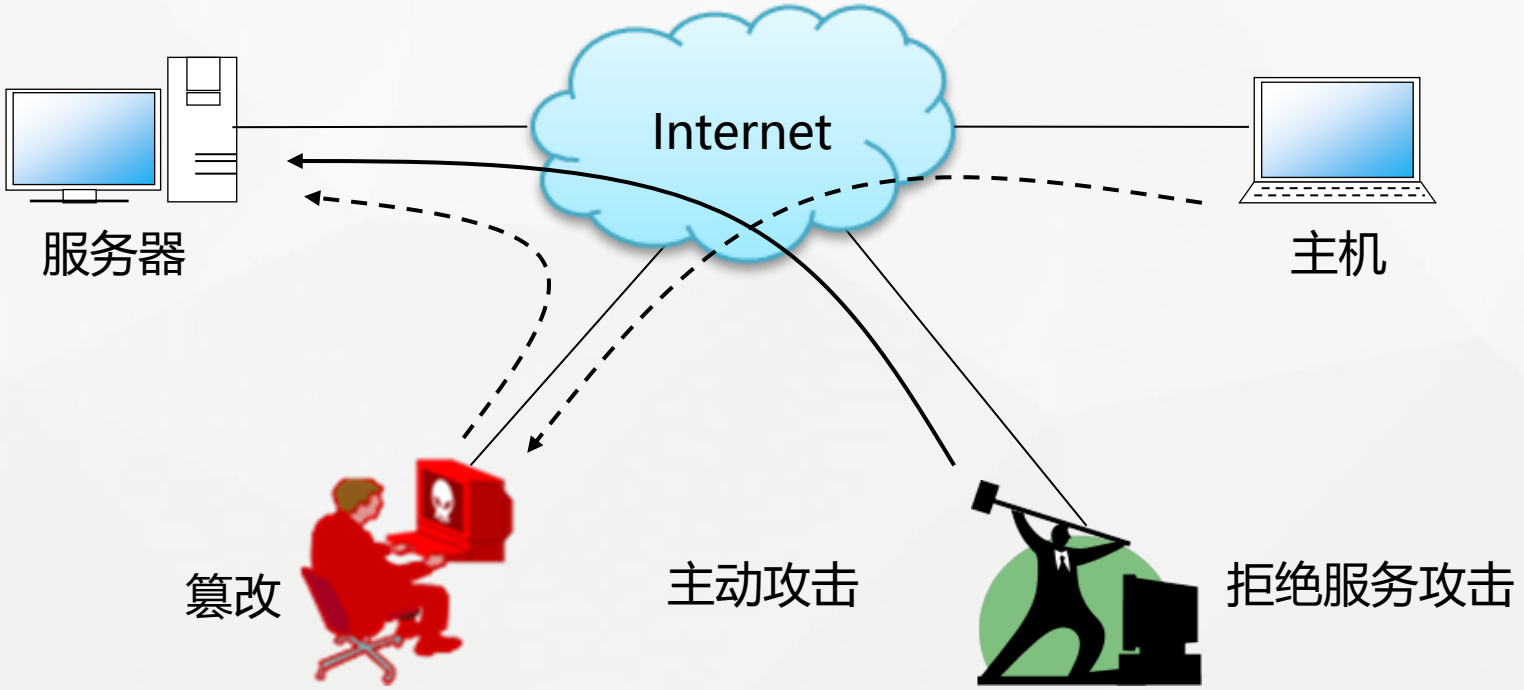
传输层：SYN Flood攻击

应用层：缓冲区溢出、漏洞、病毒及木马

网络攻击方式

被动攻击方式

网络攻击方式



主动攻击方式

常见网络攻击方式防范

网络基础

目录
Contents

学习目标

- 了解常见网络攻击方式
- 了解常见网络攻击防范方式

常见网络攻击方式

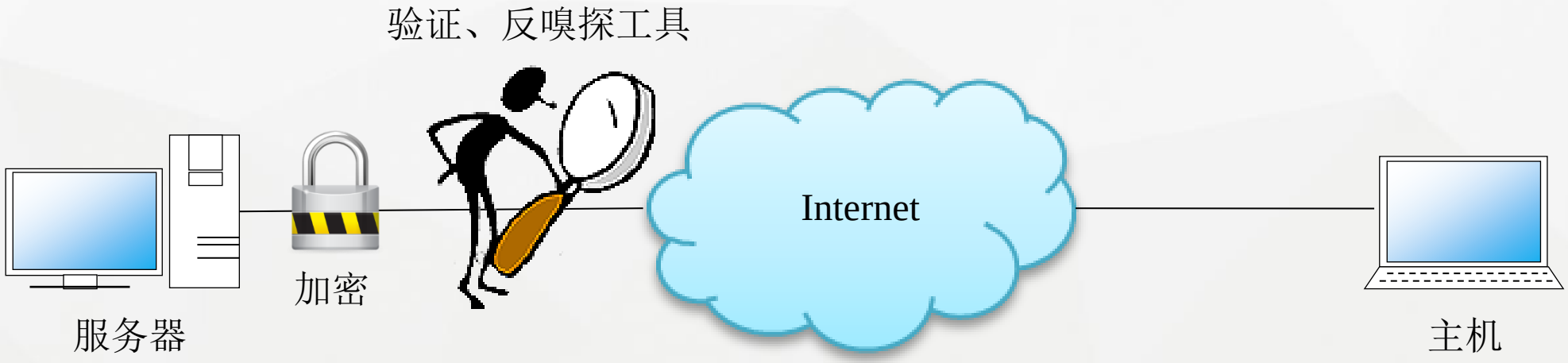
数据嗅探

数据嗅探：攻击者并不直接入侵目标系统，而是通过窃听网络来获取重要数据或信息。嗅探技术是黑客和网络管理员最常用的工具和技术。

嗅探方式	主要操作方式	常用软件
抓取报文（抓包）	通过网络监听非法获取用户信息，如明文传输的用户名、密码。抓包实际上是在以太网卡处于混杂状态下通过专门的软件实现对数据包的获取过程，通常需要与端口镜像、HUB、分光器、TAP（Test Access Point）等紧密配合。	WireShark、OmniPeek
扫描	通过发送报文探测网络中各种主机和服务的状态，准确的了解网络中的资产和系统漏洞。一般分为端口扫描和漏洞扫描。	NMAP（远程扫描工具）、Nessus（漏洞扫描工具）
操作系统标识	通过Banner Grabbing获取操作系统的各种信息，根据这些系统对包的回应的差别，推断出操作系统的种类。	NMAP（远程扫描工具）
电磁捕捉	电磁捕捉通过捕捉屏幕、网线发出的电磁波，还原信息的嗅探手段，常用于攻击军事机构。	_____

数据嗅探防范方式

数据嗅探防范方式主要有：验证、改变网络结构、反嗅探工具、加密



数据嗅探防范方式

非法使用

非法使用：指资源被未授权的用户（非法用户）或以未授权方式（非法权限）使用。

非法使用典型方式有电子欺骗、暴力攻击、权限提升、系统重启攻击等方式。

非法使用的防范方式

过滤：使用访问控制技术可以对非法IP进行严格的控制。

验证：采用非IP地址的方式强验证是防止基于非IP欺骗的最有效的技术，结合应用权限控制，还可以为溯源提供依据。

加密：对于针对密码的攻击方式，只要加密算法足够“强壮”同时采用强密码，任何攻击都是没有实效的。

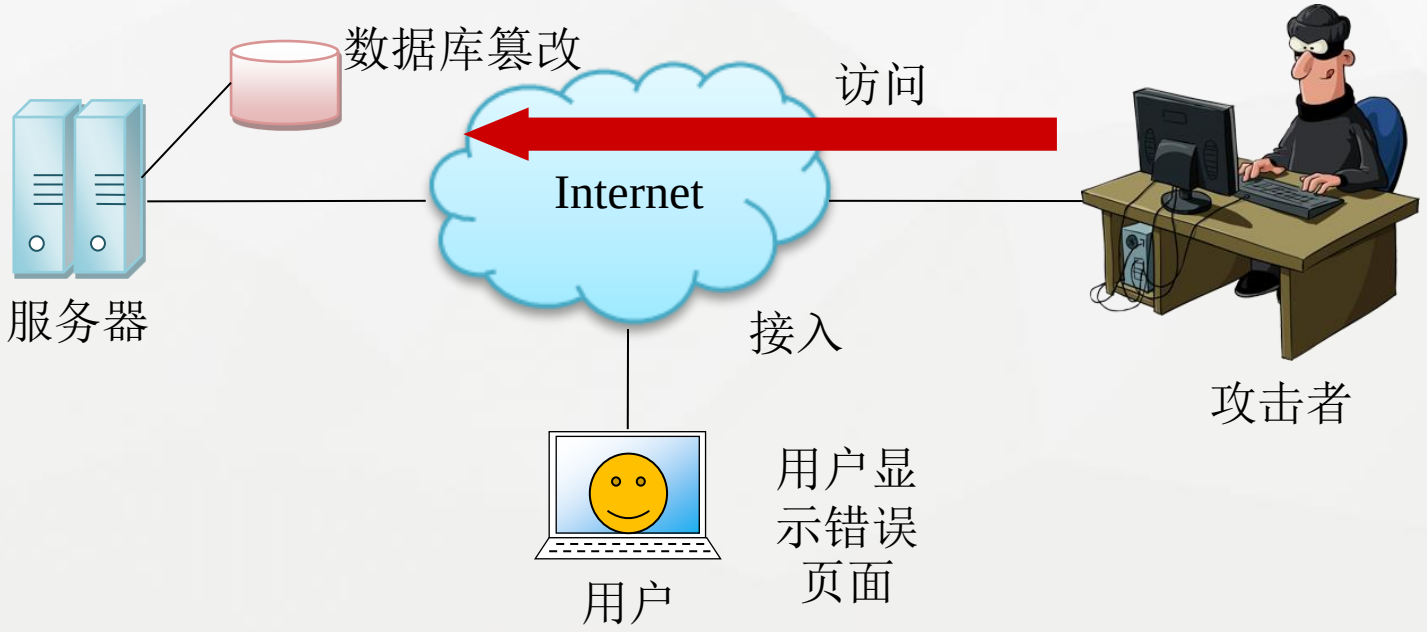
关闭服务和端口：服务和端口在为用户提供支持平台和接口时，也成为攻击者的目标，因此关闭不需要的服务和端口是非常有必要的。

信息篡改

信息篡改：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重 要信息，其目的是取得有益于攻击者的响应。

如报文重放、会话劫持、篡改审计数据、主页篡改等方式。

这类攻击防范的主要方式是数据加密。

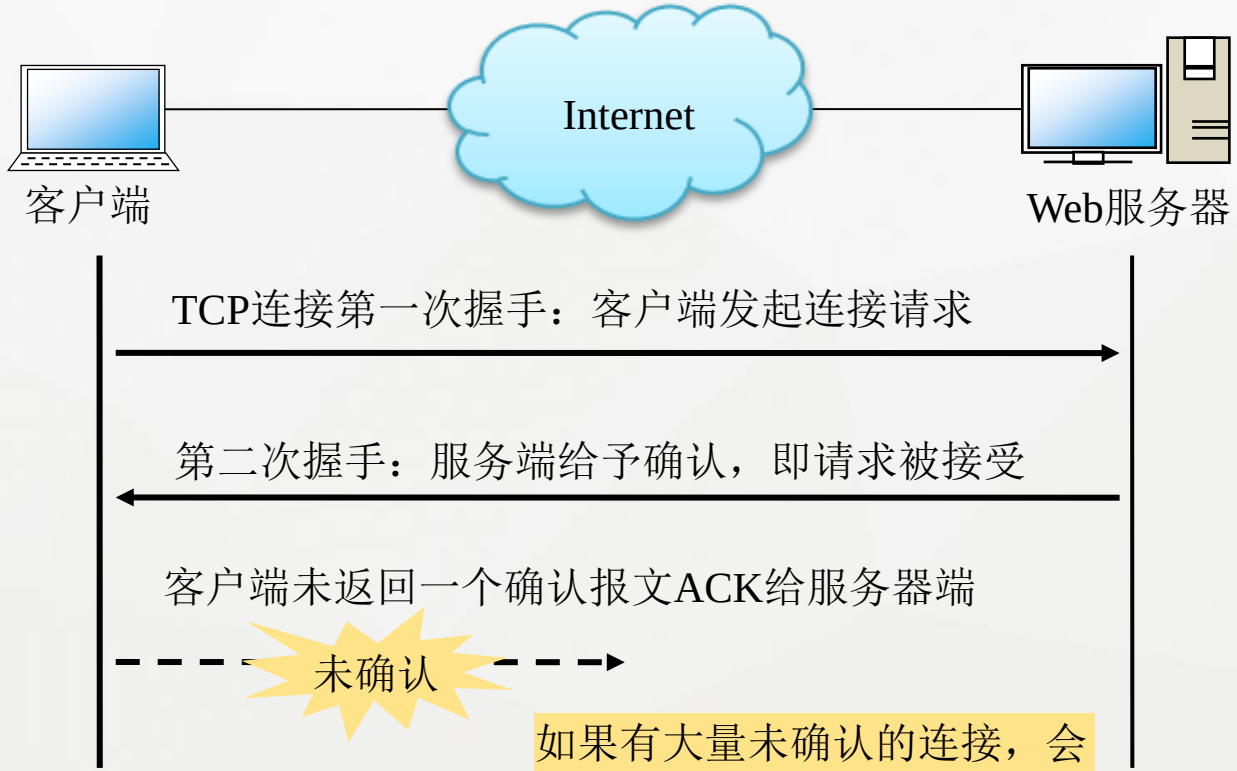


主页篡改

拒绝服务

拒绝服务DoS（Denial of Service）：是网络上一种简单但十分有效的破坏性攻击手段，通过发送大量攻击报文导致网络资源和带宽被消耗，从而达到阻止合法用户对资源的访问。

SYN Flood攻击原理



拒绝服务的防范方式

屏蔽IP：在服务器或路由器上用ACL屏蔽攻击者IP后就可以有效的防范DoS的攻击。

协议防范：根据DoS攻击每个协议的弱点进行对应的修复方法。

侦测：对DoS攻击的侦测和区分是处理DoS攻击的重要依据。当发现有特大型的TCP和UDP数据包通过或数据包内容可疑时都要注意。

BUG和恶意代码

BUG：是一个程序（代码）的漏洞，它会产生一个隐藏的通道。很多情况下一个运行在服务器的操作系统或程序都会出现这些问题，攻击者经常研究并充分利用它们。两种常见的BUG：后门（Backdoor）、缓冲区溢出（Buffer Overflow）。

恶意代码（Malicious code）：是攻击设备、用户、系统、网络的软件统称。常见恶意代码包括病毒、蠕虫、木马等。

访问控制

网络基础

目录

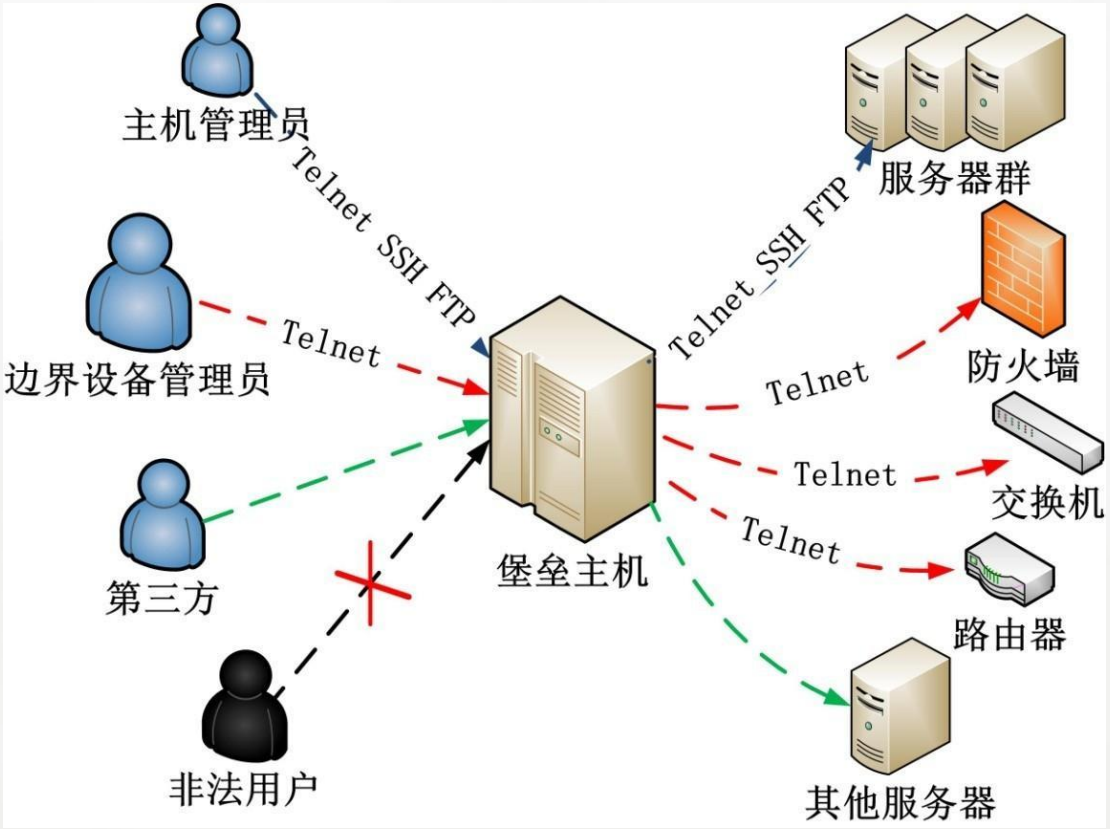
Contents

学习目标

- 了解什么是访问控制及其作用
- 熟悉访问控制策略的几种方式

访问控制作用

访问控制：是策略和机制的集合，它允许对限定资源的授权访问。它也可保护资源，防止那些无权访问资源的用户的恶意访问或偶然访问。



访问控制策略方式

访问控制策略：主要是根据用户的身份及访问权限决定其访问操作，只要用户身份被确认后，即可根据访问控制表上赋予该用户的权限，进行限制性地访问。

访问控制策略的三种方式

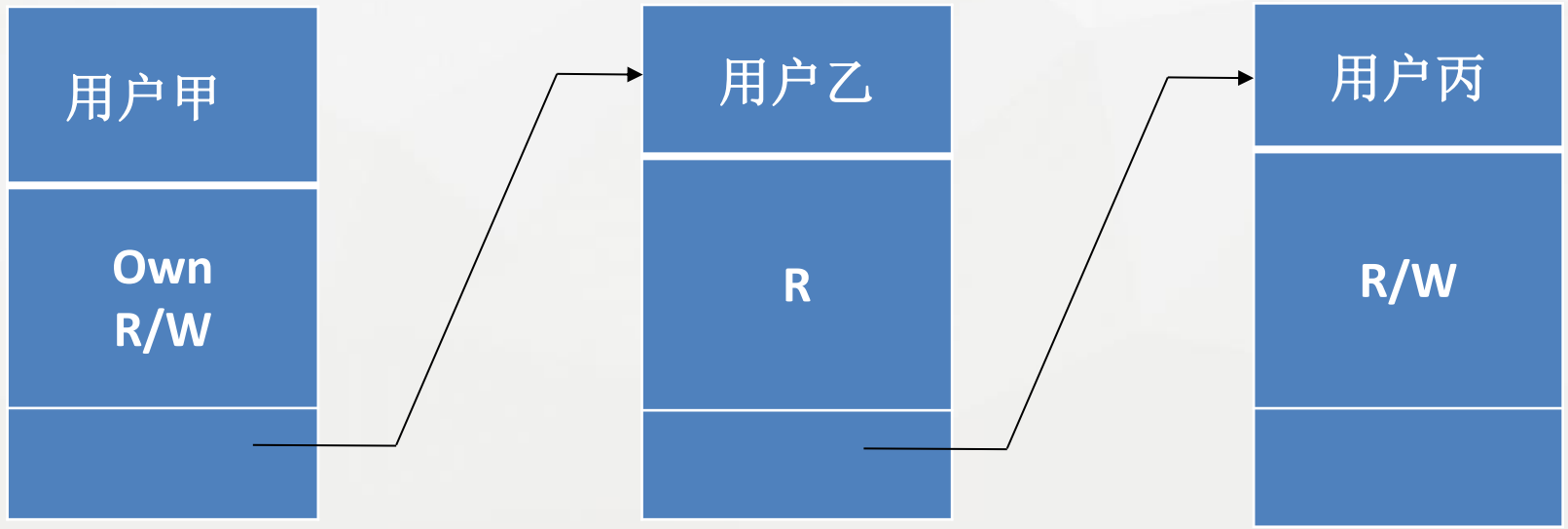
（1）访问控制矩阵（Access Contro1 Matrix）

访问控制矩阵就是确保系统的操作是按照访问控制矩阵授权的访问来执行，它是通过引用监控器，来协调客体对主体的每次访问，这种方法清晰的实现认证与访问控制的相互分离。

	文件A	文件B	文件C
用户甲	Own/R/W	R/W	R
用户乙	R	Own/R/W	R/W
用户丙	R/W	R	Own/R/W

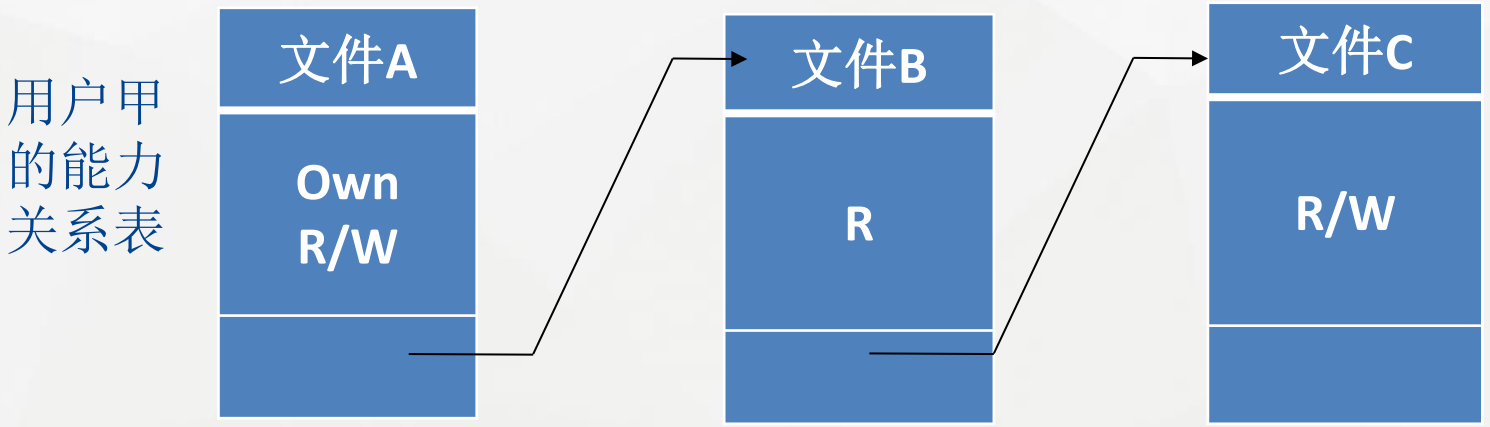
（2）访问控制表（ACL， Access Control List）

访问控制表是以资源为中心建立访问权限表。在访问控制表中记录了某文件被授权访问的用户名及访问权的隶属关系。通过查询访问控制表，能够很清晰准确地查找出对于特定内容的授权访问，用户可以访问哪些内容并有什么访问权限。



（3）能力关系表（Capabilities Lists）

能力关系表与ACL相反，是以用户为中心建立访问权限表，表中规定了该用户可访问的文件名及访问权限，利用能力关系表可以很方便查询一个用户的所有授权访问。



入侵检测防御技术

网络基础

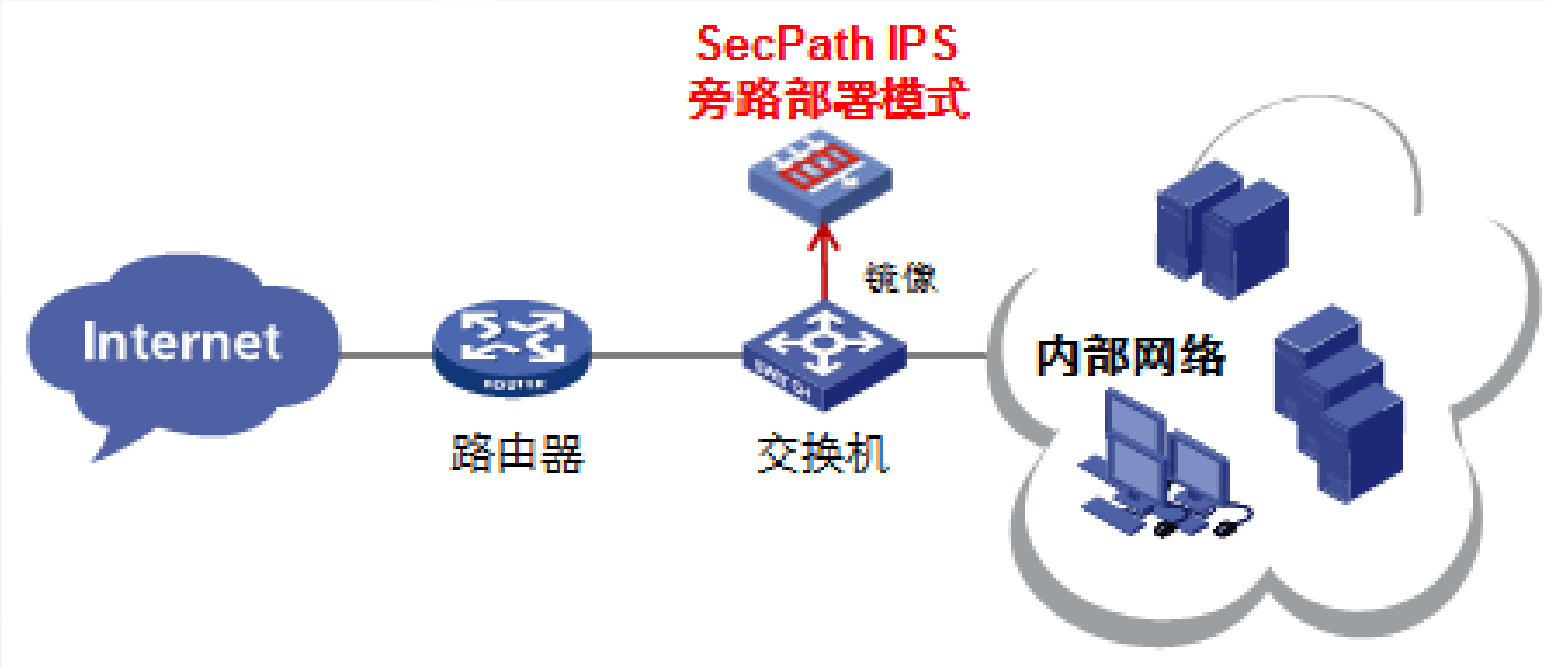
目录

Contents

学习目标

- 了解什么入侵检测防御技术
- 熟悉入侵检测系统、入侵防御系统及其区别

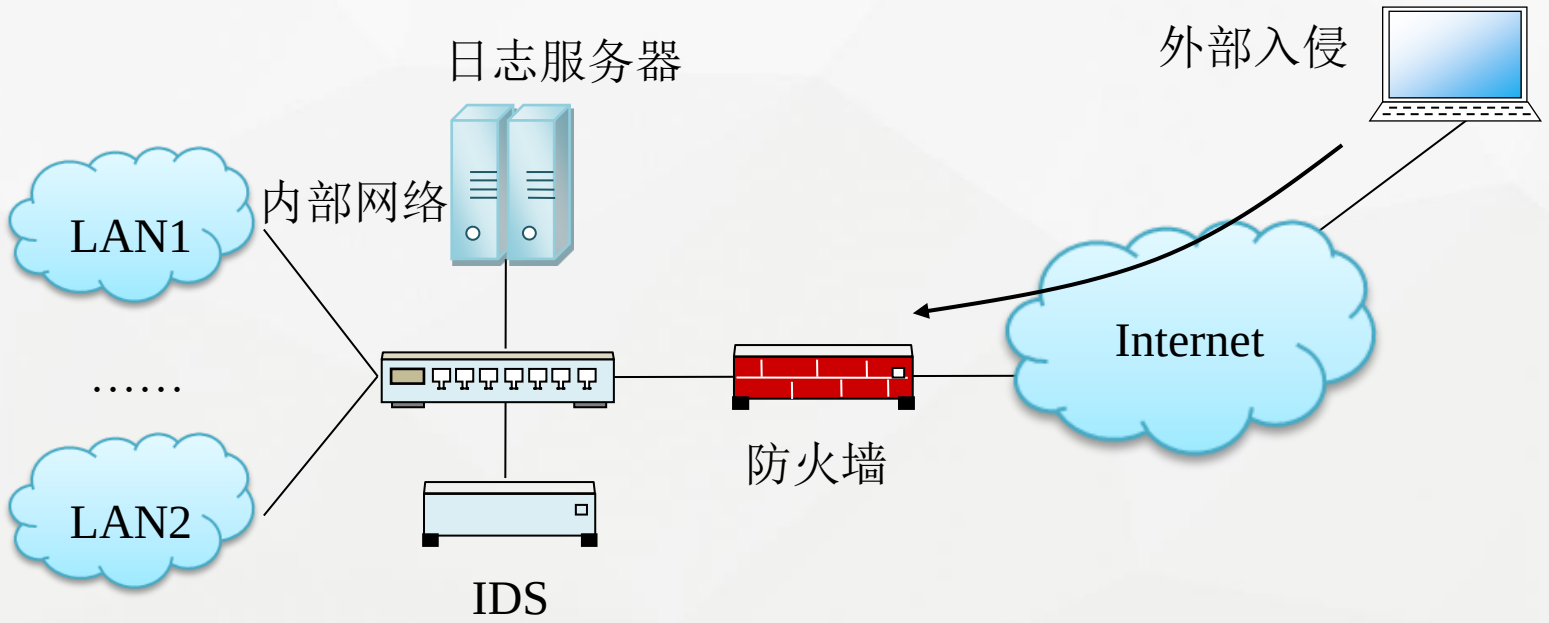
入侵检测防御技术：指识别针对计算机或者网络资源的恶意企图和行为，并对此做出反应的一种网络技术。



入侵检测防御技术可以通过入侵检测系统和入侵防御系统实现。

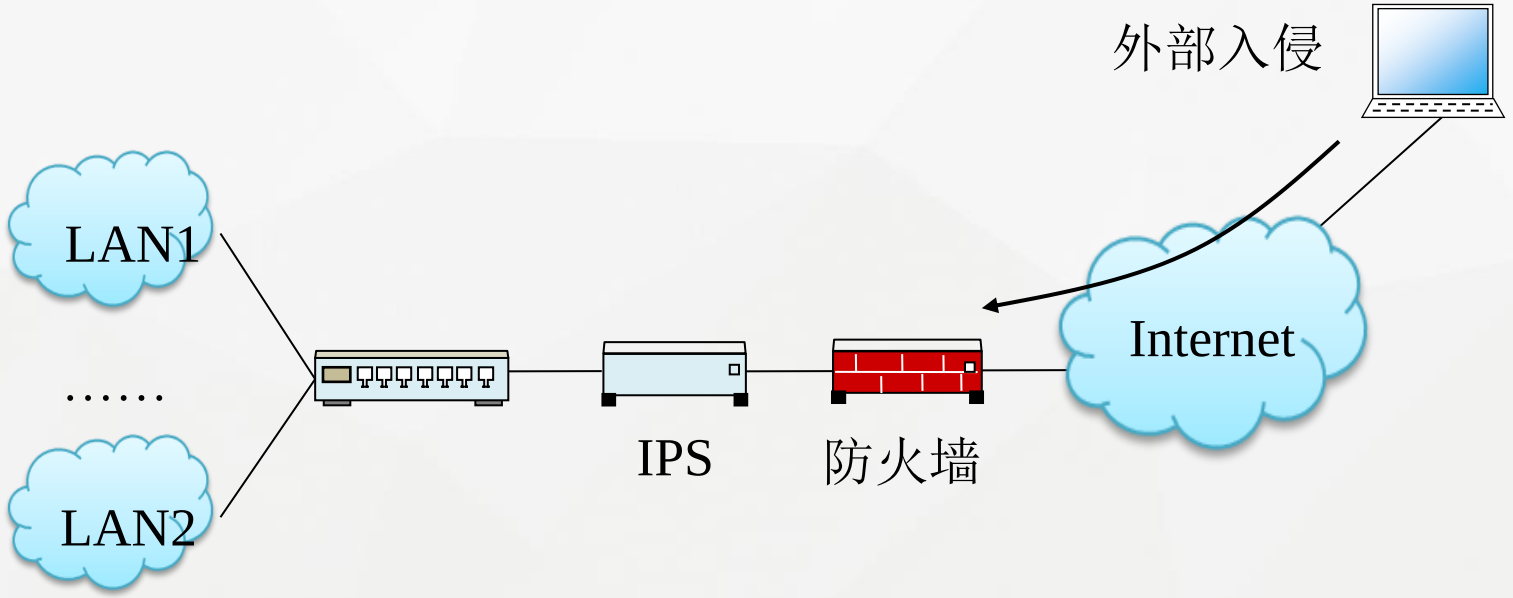
入侵检测系统

入侵检测系统（IDS，Intrusion Detection System）就是对入侵行为的发觉，担负着保护整个网段的任务。



入侵防御系统

入侵防御系统（IPS， Intrusion Prevention System ）检测是指针对检测到的网络中的攻击进行主动防御，在IPS设备上对攻击流进行处理。



IPS和IDS区别：两者的部署方式不同，IDS为旁挂方式，对网络影响比较小，而IPS采用直路的方式，加入了单点故障，同时IPS设备的性能对网络也有比较大的影响。

内网安全解决方案

网络基础

目录

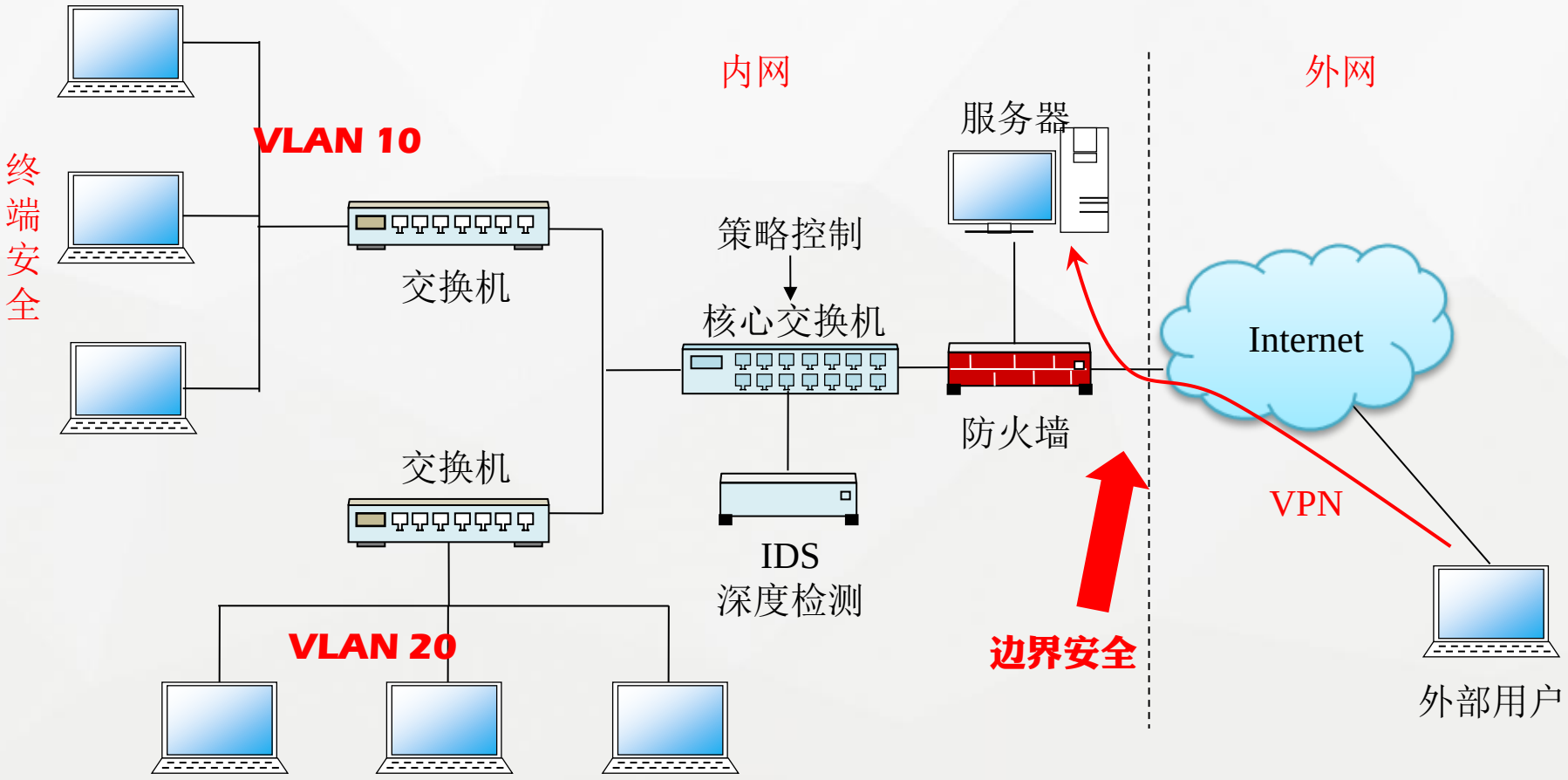
Contents

学习目标

- 理解内网安全解决方案的三个方面：边界安全、业务安全和终端安全

内网安全解决方案

内网安全解决主要包含三个方面：边界安全、业务安全、终端安全



边界安全

边界防御可以抵御大部分外网攻击，而合理的网络架构是构建边界防御的前提条件。另外需要进行风险评估，要明确企业自己的内网可能面临哪些风险，现有条件下对这些风险的承受程度如何。

（1） 在网络出口部署防火墙，入侵检测设备，降低外网对内网的安全威胁；

（2） 部署VPN，确保移动用户身份的合法性；

（3） 在内部网络中，将不同业务类型的用户组划分在不同的Vlan，在Vlan间访问进行访问策略限制。

业务安全：

在企业网络中存在的计费系统，VOIP，带宽管理等类型的业务，如何保证不被非法使用保证企业的收益是至关重要的；在P2P，游戏，IM（Instance Message）等业务流行的网络环境中，如何保证带宽合理应用、员工高效率的工作，也是企业领导关心的问题。针对业务安全的典型技术就是深度检测技术。

终端安全：

从某种意义上来说，网络上所有不安全的因素都来自人员。据ISCA（International Symposium on Computer Architecture）统计，全球每年仅仅由于信息安全问题导致的损失高达数百亿美元，其中来至于内部的威胁高达60%，来自内部的威胁已经成为企业首要的安全问题。终端安全包含终端设备的安全和终端用户行为安全。

加密技术概述

网络基础

目录

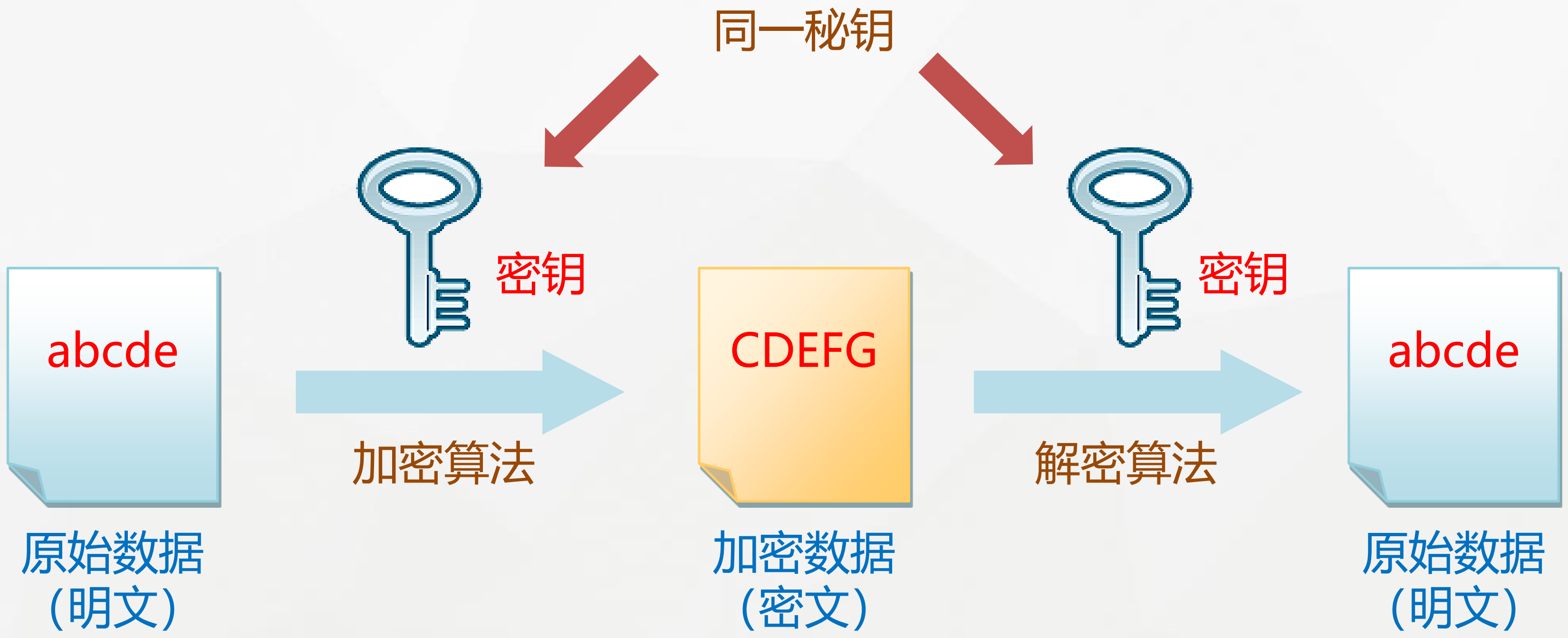
Contents

学习目标

- 熟悉加解密相关的概念
- 了解加解密过程
- 熟悉对称加密和非对称加密技术

加解密过程

加密是指利用某个数值（密钥）对明文的数据通过一定的算法变换成加密（密文）的数据过程。



转换取决于这个密钥。

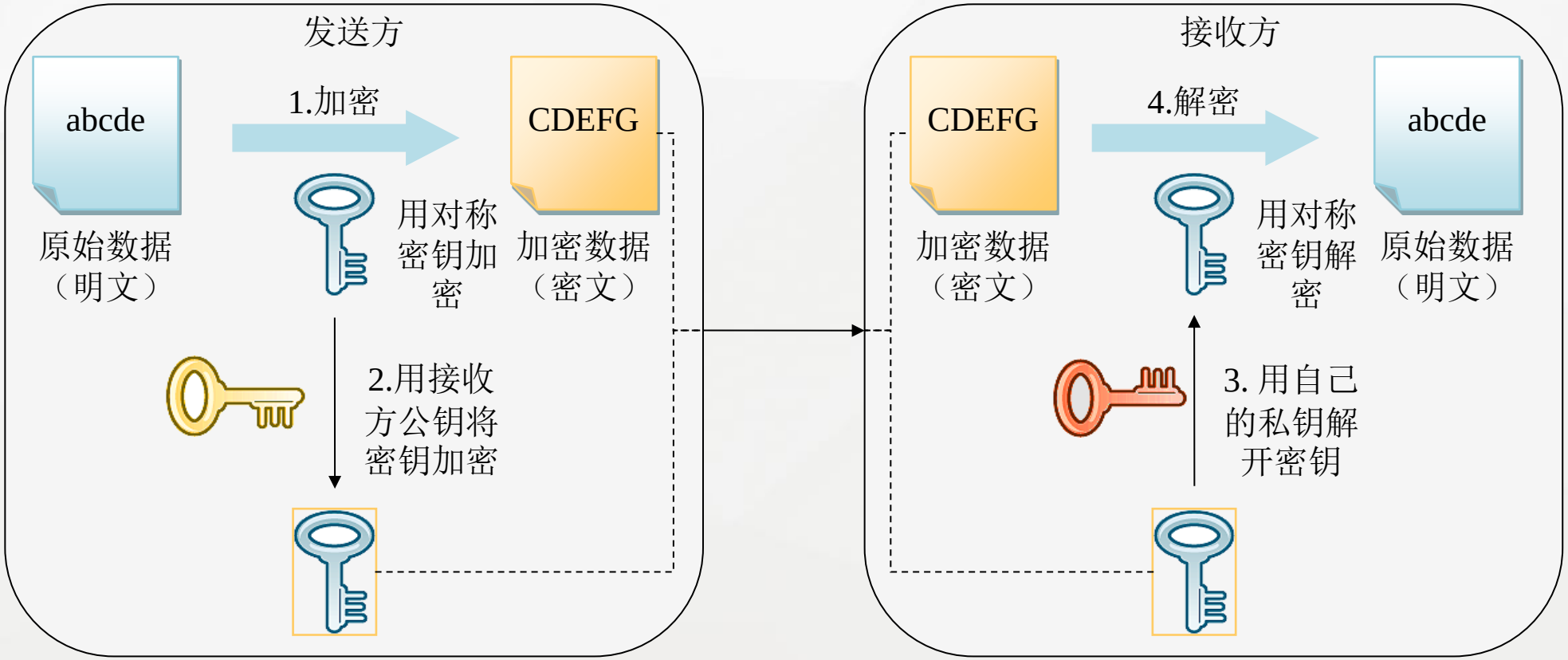
非对称加密

非对称加密：在加密和解密的过程中分别使用不同的密钥叫做非对称加密方式

若使用私钥进行加密，则需要使用公钥解密。

密钥交换技术

密钥交换技术：是一种混合加密方式，发送方和接收方使用对称加密方式，为保证密钥传输的安全性，对密钥使用非对称加密方式进行传输。



数字签名

网络基础

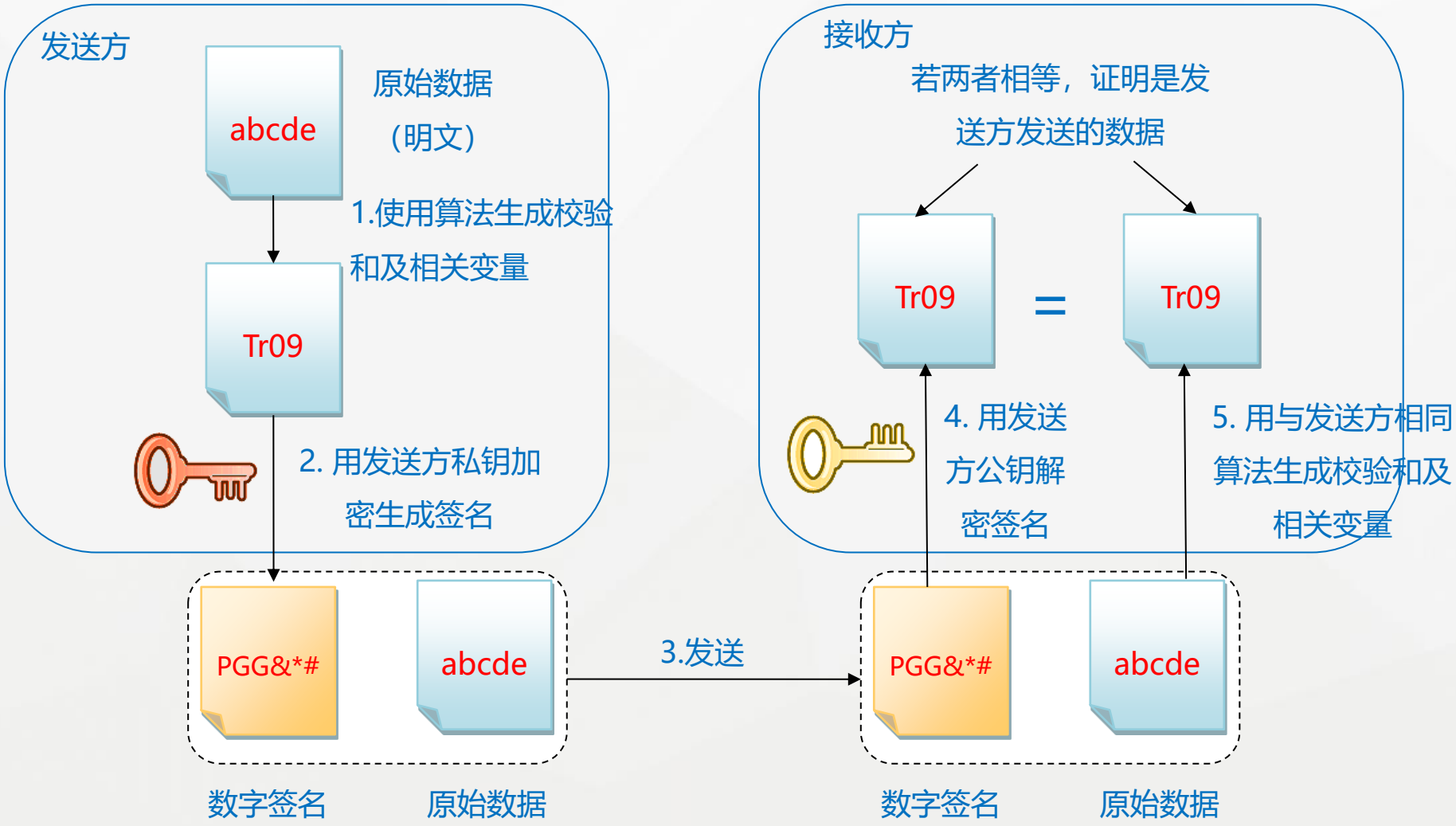
我们收到的文档可信吗？

网络钓鱼

网络诈骗

数字签名

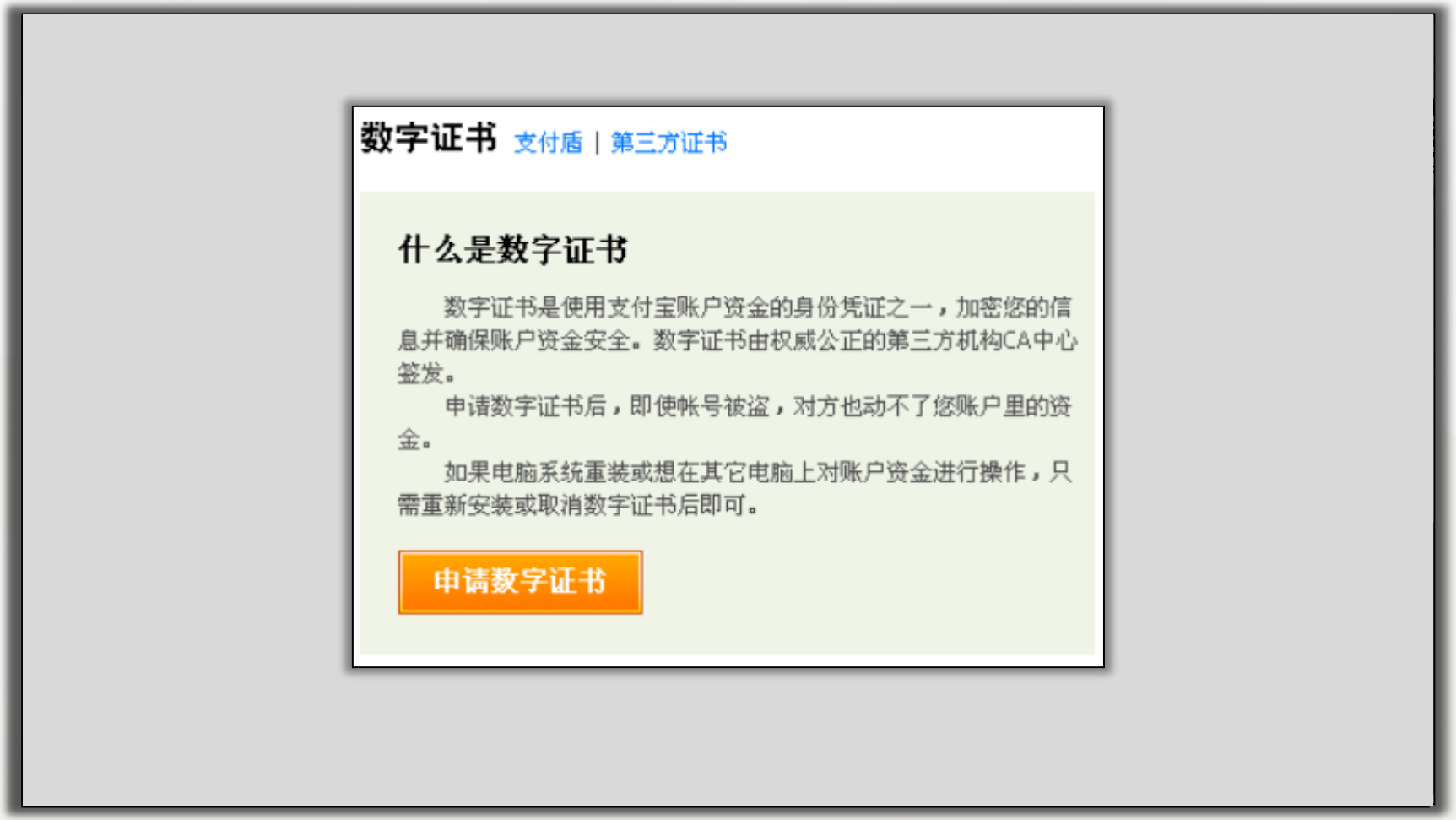
保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生

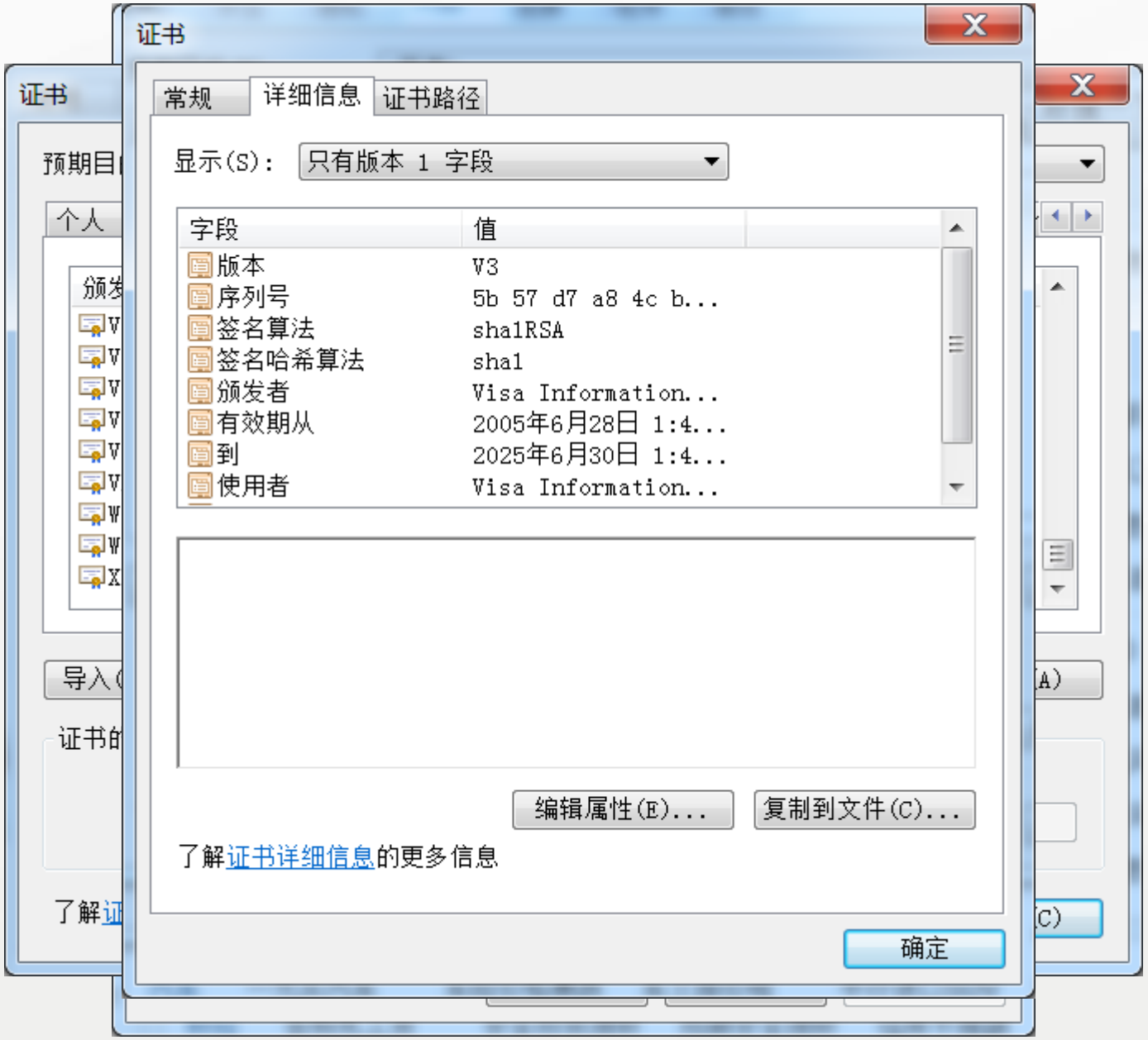


数字证书

网络基础

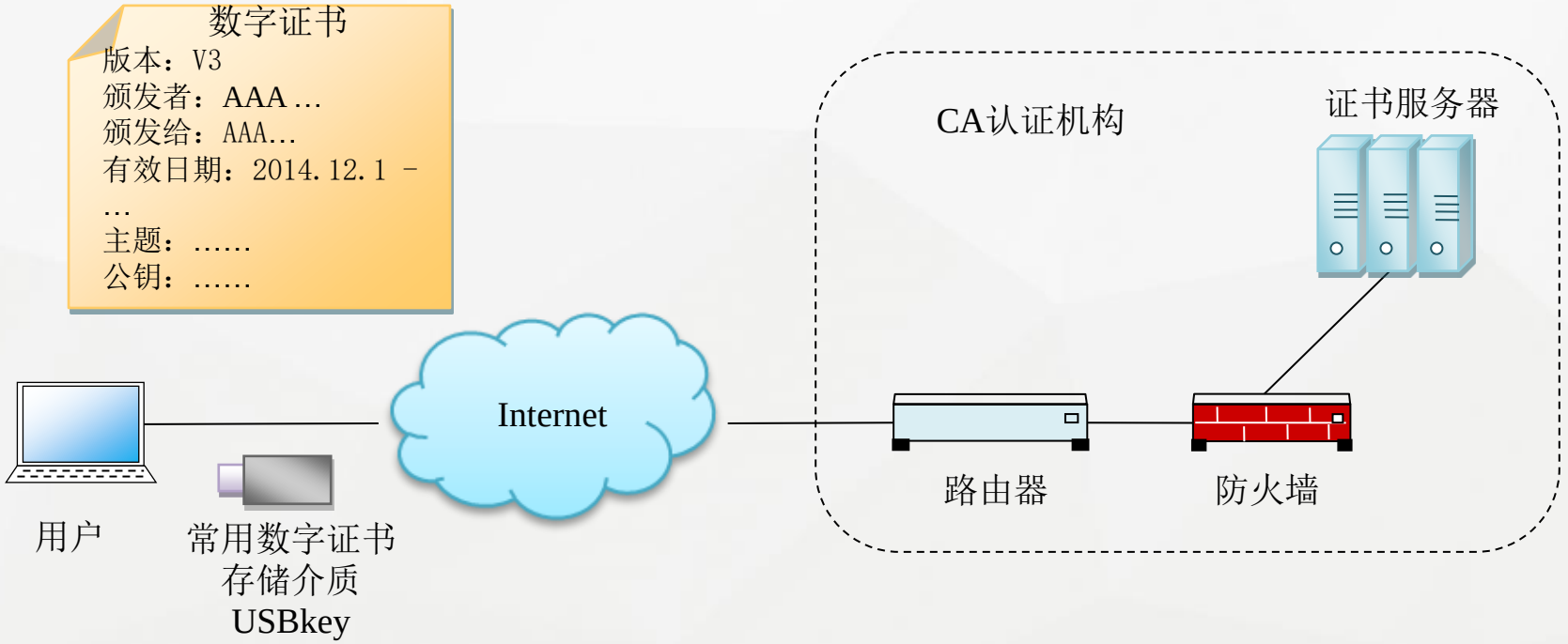
如何保证网络交易的安全性?




证书
常规
详细信息
证书路径
显示(S)：
只有版本 1 字段
字段
值
版本
V3
序列号
5b 57 d7 a8 4c b...
签名算法
sha1RSA
签名哈希算法
sha1
颁发者
Visa Information...
有效期从
2005年6月28日 1:4...
到
2025年6月30日 1:4...
使用者
Visa Information...
编辑属性(E)...
复制到文件(C)...
了解证书详细信息的更多信息
确定

数字证书

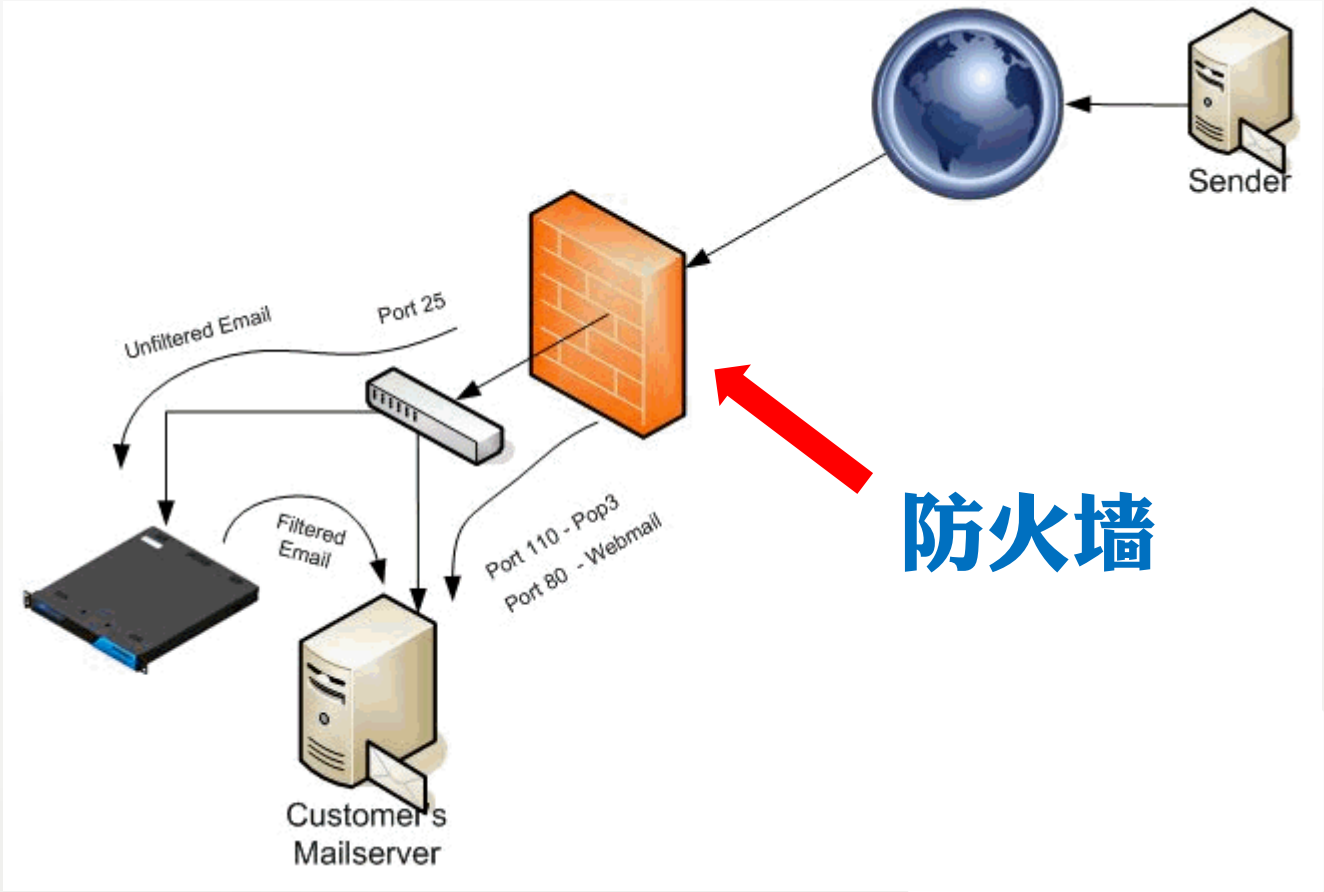
数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。



防火墙基本功能

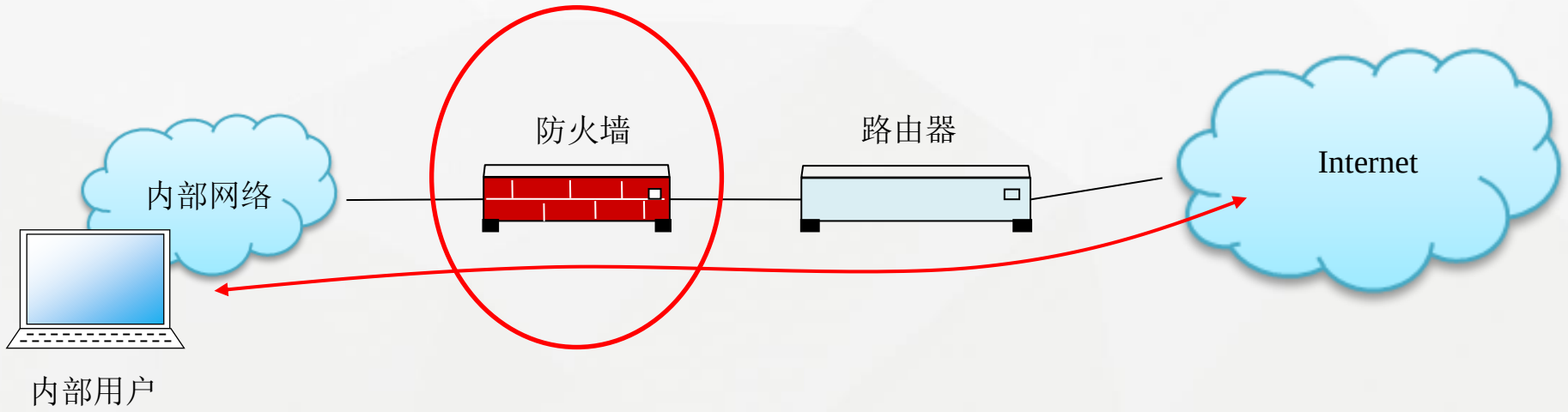
网络基础

如何保证内部网络不收外来攻击?



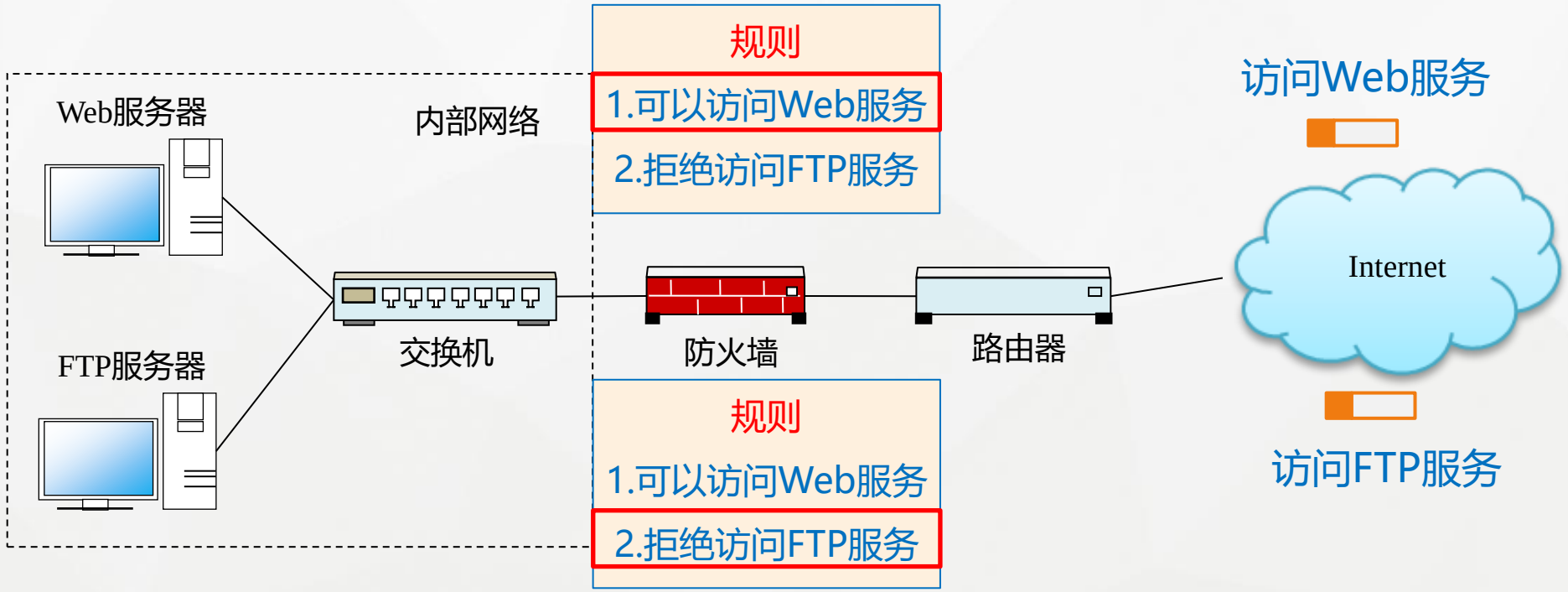
防火墙基本功能

1.内部网络和外部网络之间的所有网络数据流都必须经过防火墙



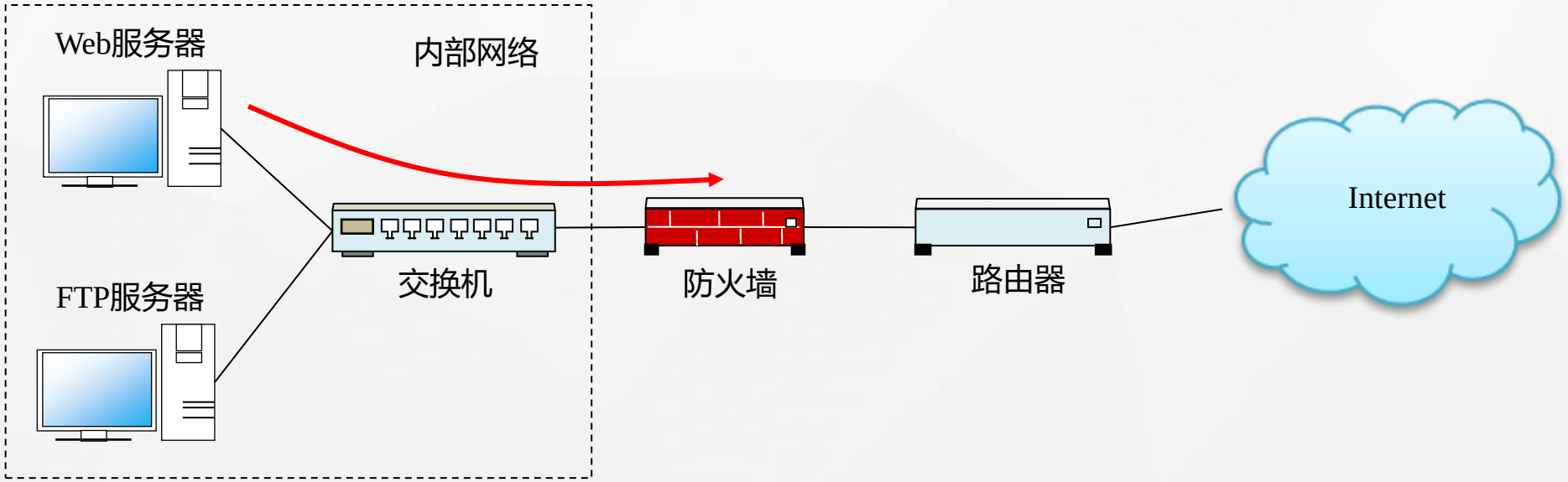
防火墙基本功能

2.只有符合安全策略的数据流才能通过防火墙



防火墙基本功能

3.防止内部信息的外泄

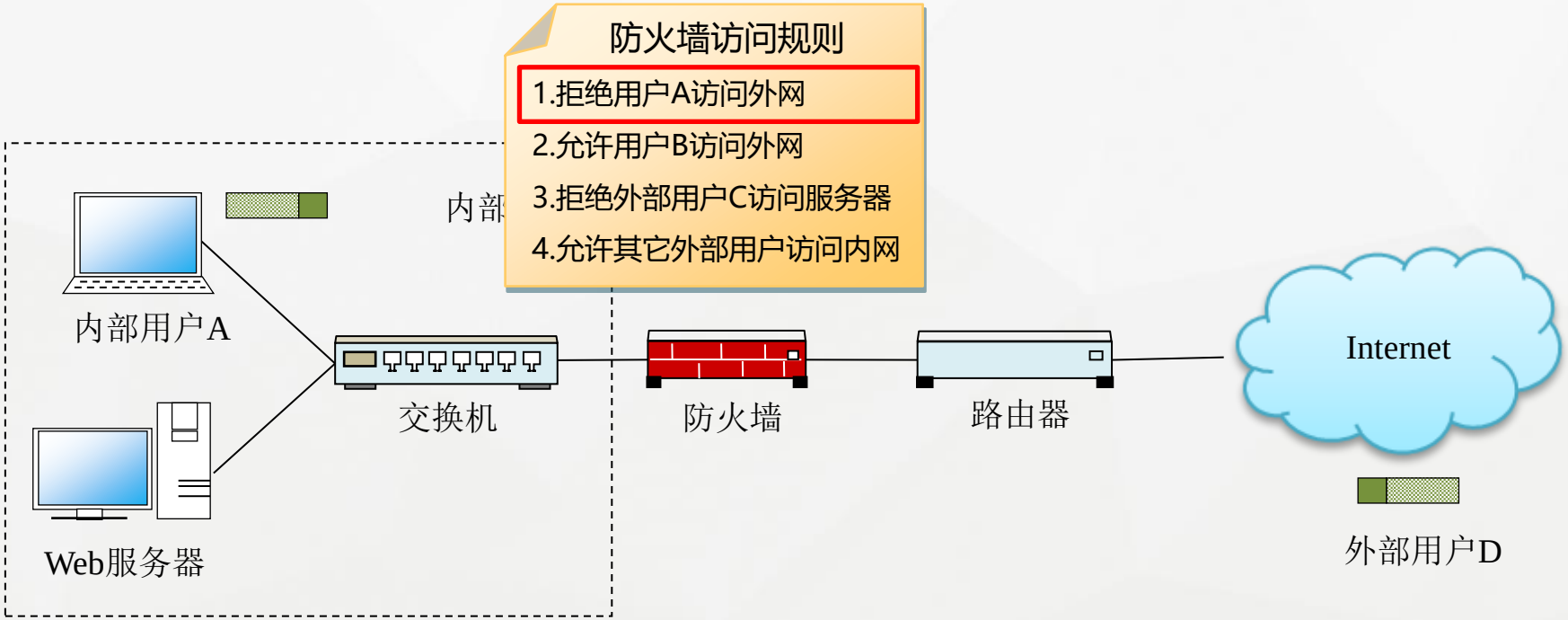


防火墙的分类

网络基础

1.包过滤防火墙

包过滤是指在网络层对每一个数据包进行检查，根据配置的安全策略转发或丢弃数据包。

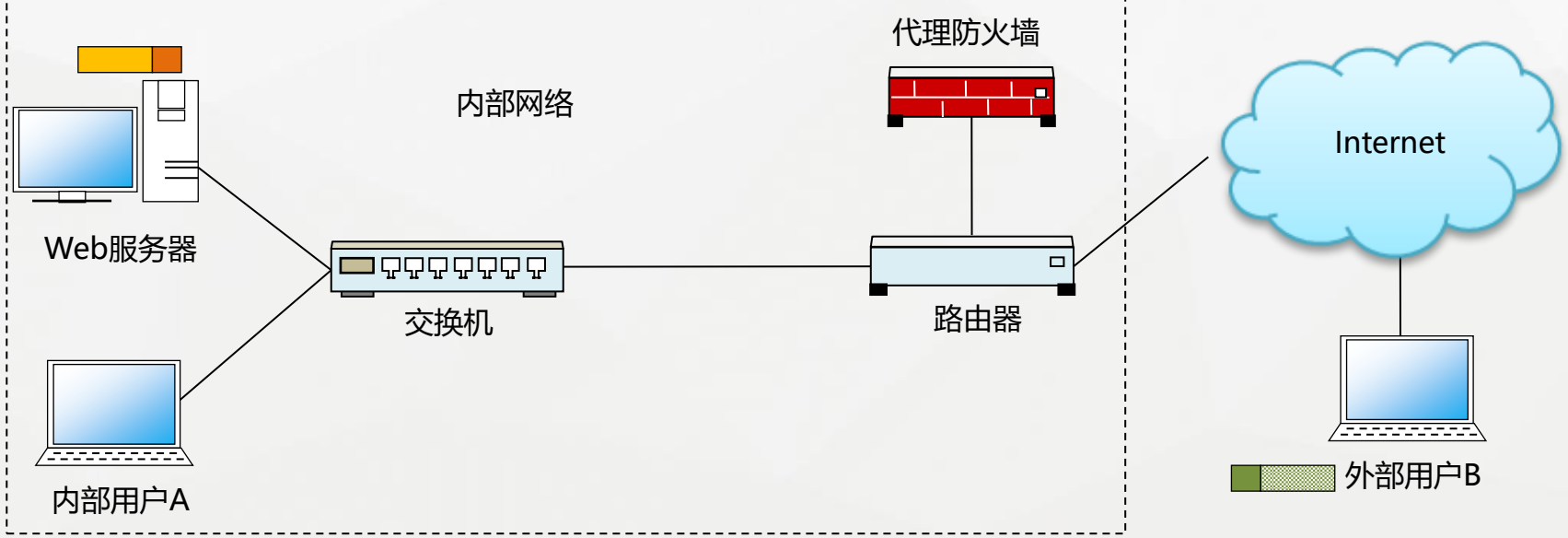


2. 代理防火墙

代理防火墙实质是把内部网络和外部网络用户之间直接进行的业务（访问）由代理接管。

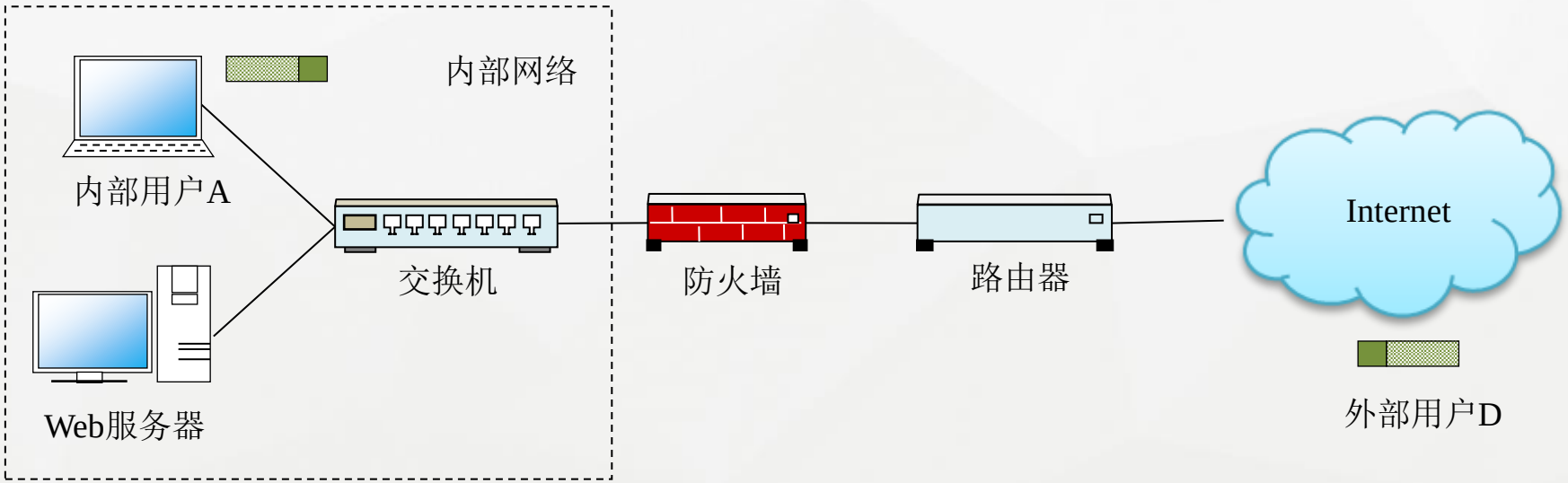
代理防火墙首先检查外部用户的请求，

通过后，其代理发起与内网的连接



3.状态监测防火墙

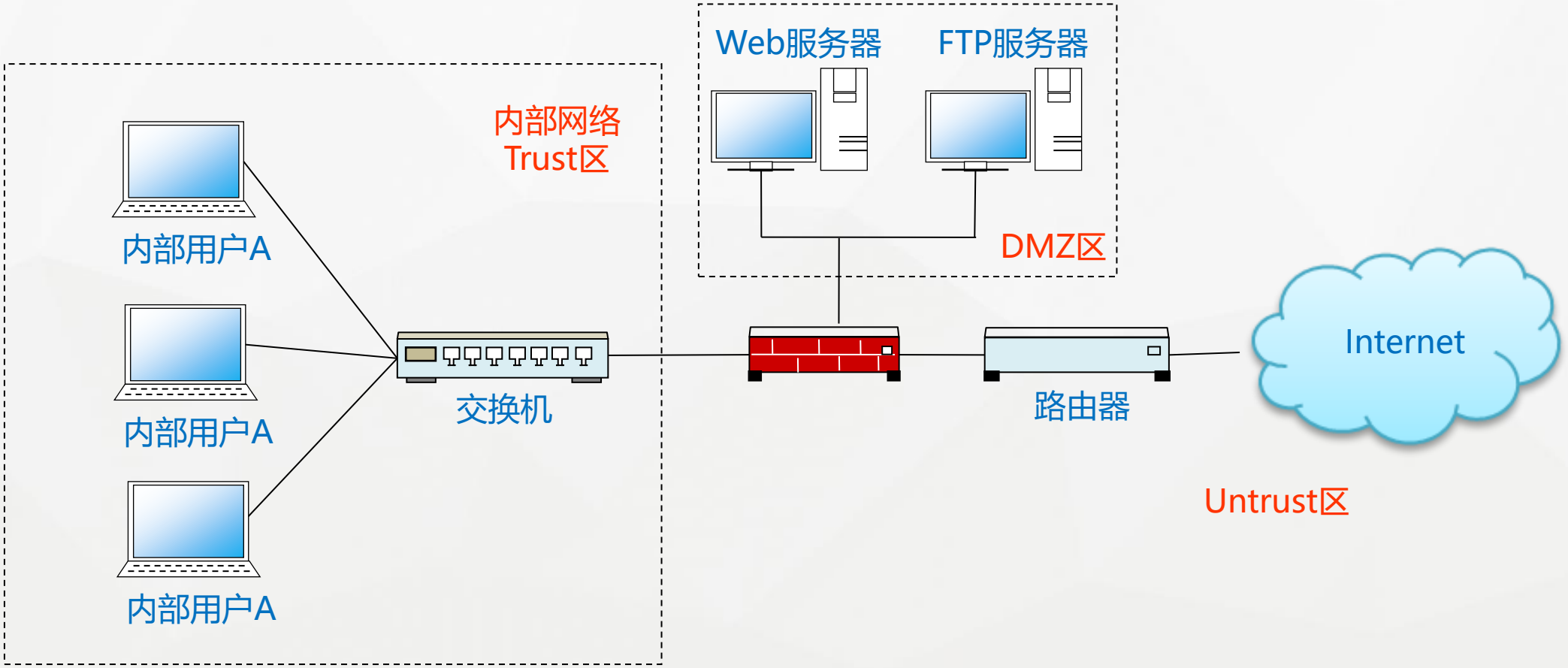
通过通信的状态检验数据报文的合法性，属于深度监测。



网络中防火墙部署方式

网络基础

防火墙部署方式


Web服务器
FTP服务器
内部网络
Trust区
DMZ区
内部用户A
内部用户A
内部用户A
交换机
路由器
Internet
Untrust区

谢谢

Thanks!