✏️ by kingno

9. PKI&PMI

9.1 PKI 的基本概念

9.1.1 基本概念

- PKI：公钥基础设施(Public Key Infrastructure), 是利用 公钥理论和技术 提供安全服务的基础设施
- PKI 的目的：解决网上身份的 完整性 和 不可抵赖性 等安全问题
- PKI 的任务：确立可信任的 数字身份

9.1.2 PKI 的组成

1. 证书机构（CA）：负责 管理 和 签发 数字证书
2. 注册机构（RA）：数字证书审批机构（CA签发后要经过RA审批）
3. 证书发布库：用于存储 已签发 的数字证书及公钥
4. 密钥备份及恢复系统：它可以备份和恢复加/解密密钥， 无法对签名密钥进行备份
5. 证书撤销系统：在证书有效期内作废证书
6. 应用接口（API）：使用户能够方便地使用加密、数字签名等安全服务

9.2 数字证书

9.2.1 基本概念

数字证书的概念：一个用户的身份信息与其公钥相结合形成未签名的证书，再由一个权威机构来证实用户的身份，最后由该机构对未签名的证书进行数字签名

9.2.2 数字证书的生成步骤

> 参考教材《计算机安全原理与实践》

1. 用户创建一对密钥：一个公钥，一个私钥
2. 客户端准备一个包含用户ID和公钥的未签名的证书
3. 用户通过某种安全手段将未签名的证书提交给CA
4. CA以如下方式产生一个签名：
   - 首先，CA利用某个散列函数计算出未签名证书的 散列码
   - 然后，CA用自己的 私钥 对散列码进行加密，以此产生一个签名
5. CA将签名附属在未签名的证书后，以此创建一个签名证书
6. CA将签名证书交还给客户端
7. 客户端可以将该签名证书提交给其他用户
8. 该签名证书的任何接收者可以通过如下方法验证该证书的有效性：
   1. 接收者计算证书的散列码（即未签名的证书的散列码）
   2. 接收者用已知的 CA的公钥 对签名进行 解密
   3. 接收者比对（1）和（2）中的结果，如果匹配，那么证书是有效的

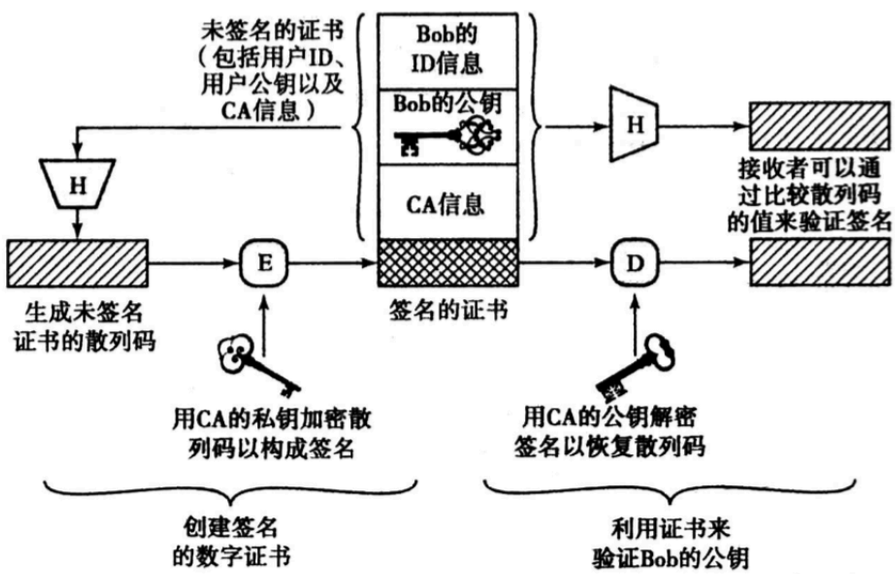


图 2-7　公钥证书的使用

9.3 PKI 体系结构——PKIX 模型

- 公钥基础设施X.509(PKIX) 适用于在Internet上部署X.509公开密钥（X.509是一种标准）
- PKIX定义了公钥基础设施的大部分功能

9.5 授权管理设施 PMI

9.5.1 基本概念

授权管理设施用来实现权限和证书的产生、管理、存储、分发和撤销等功能

9.5.2 与 PKI 的区别

- PKI 证明用户 是谁 ，并将用户的身份信息保存在用户的公钥证书中
- PMI 证明这个用户 有什么权限 、什么属性、能干什么，并将用户的属性信息保存在授权证书中。它的最终目标就是提供一种有效的体系结构来管理用户的属性
- PMI 建立在 PKI 提供的可信身份认证服务的基础之上

---

10. Securities of Lower-layer Protocols

10.1 基本协议

10.1.1 IP协议的安全性

- IP 协议 不能保证 数据就是从数据包中给定的源地址发出的
- IP 欺骗攻击：攻击者可以发送含有 伪造返回地址 的数据包
- 当路由器遇到 大流量 的情况下，会丢失数据包

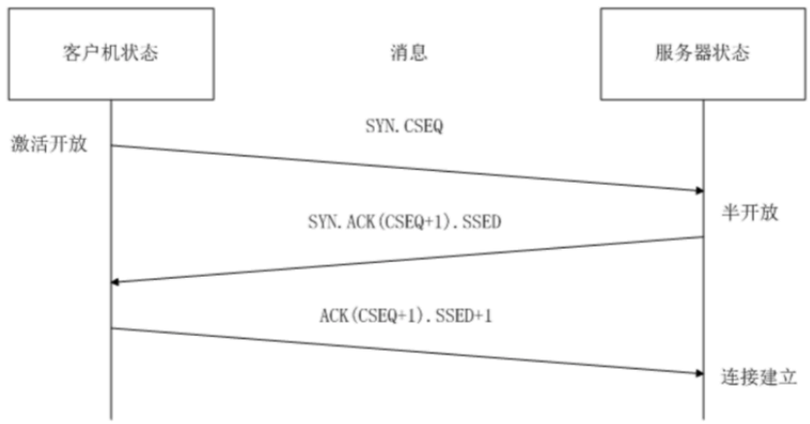
- 大数据包可能在中间节点上被拆分为小数据包。通过向包过滤器注入大量病态的小数据包，可以对包过滤器造成破坏

10.1.2 ARP 协议的安全性

ARP 协议用于确定 IP 地址和 MAC 地址的映射

- ARP 欺骗攻击：一台计算机会发出假冒的 ARP 查询或应答信息，并将所有流向它的数据流转移，这样它就能伪装成某台机器，或修改数据流

10.1.3 TCP 的安全性



- SYN Flood 攻击：攻击者利用服务器的半开放状态发动攻击。攻击者发送大量 SYN 数据包，但是不进行第三步的 ACK 回应，使服务器一直处于半开放状态，导致其他用户得不到正常的响应

  防范措施：1. SYN Defender 2. SYN proxy

- 序号攻击：如果攻击者能够预测目标主机选择的起始序号，它就能欺骗该目标主机，使其相信它正与一台可信的主机会话

10.1.4 UDP 协议的安全性

- 缺少流控：容易造成丢包
- 没有电路的概念，忽略了源地址和源端口号
- 没有握手过程，容易受到欺骗

10.1.5 ICMP 的安全性

- 一台主机所收到的ICMP消息都属于某些特定的连接。黑客会 滥用ICMP来中断这些连接
- 黑客能够利用ICMP对消息进行重定向

10.2 网络地址和域名管理

10.2.1 路由协议的安全性

- IP loose source route 选项可以使往返路径都是用户指定的。这意味着攻击者可以通过控制路由而假冒任何主机骗取信任
- 将伪造的 RIP 数据包注入网络非常容易，如果发起攻击的主机比真实的源主机离目标主机的距离更近，就容易改变数据流的方向

10.2.2 DHCP 协议的安全性

- 此协议只能用于本地网络使用，避免攻击者发起 远程攻击
- DHCP 查询没有认证措施，容易受到 中间人攻击和 DOS 攻击
- 如果攻击者已经接入到本地网络，那么它就可以对DHCP服务器发起 ARP欺骗攻击
- 会存在假冒的DHCP服务器

10.2.3 DNS 协议的安全性

- DNS 缓存污染：攻击者采用特殊的DNS请求，将虚假信息放入DNS的缓存中
- DNS 信息劫持：攻击者监听DNS会话，猜测DNS服务器响应ID，抢先将虚假的响应提交给客户端

10.3 IPv6

本质上 IPv6 并不能比 IPv4 更安全。要保证IPv6网络的安全性，仍然需要传统的安全设备，如防火墙，IDS等

10.4 网络地址转换

NAT 用于解决 IPv4 地址空间缺乏的问题

- NAT 并不能处理任意的应用协议
- NAT 最严重的问题是，不能与加密协调工作。1. NAT 不能对加密的数据流进行检查；2. IPsec 与 NAT 会产生冲突，因为IPsec要保护传输层协议头，而NAT却要重写该协议头中的IP地址

---

11. Securities of Upper-layer Protocols

没有全部整理，感觉有些不是很重要

11.1 电子邮件协议

- SMTP：它常以root用户权限工作，这违背了“最小信任”原则
- POP3：允许用户删除保存在邮件服务器上的邮件
- MIME：它可能会邮递可执行程序，会传播蠕虫和病毒

11.2 消息传输协议

- FTP 的安全性：一个伪装成 FTP 客户机的 Java 程序可以将代码嵌入到指定的 Web 页面中，当有人访问这个页面，可能造成防火墙打开某些端口

11.3 远程登录协议 Telnet

- 攻击者可以通过嗅探器记录用户名和口令组合，或者记录整个会话
- 黑客掌握了使用 TCP 劫持工具的方法，使他们能够在某种条件下霸占 TCP 会话

---

12. VPN

12.1 VPN 的基本概念

定义：虚拟专用网(Virtual Private Network, VPN)，是指将物理上分布在不同地点的网络通过公用网络连接而构成逻辑上的虚拟子网

特点：费用低、安全保障、服务质量保证、可扩充性和灵活性、可管理性

分类：网关-网关VPN 和 远程访问VPN（移动用户）

12.2 隧道协议与 VPN

- 隧道协议：指通过一个 公用网络 建立的一条安全的、 逻辑 上的隧道
- 在隧道中，数据包被重新封装发送
- VPN 的主要封装协议，第二层隧道协议：PPTP、L2TP、L2F，第三层隧道协议：IPSec、GRE

12.2.1 第二层（传输层）隧道协议

- 优点：简单易行；缺点：可扩展性不好；不提供内在的安全机制，不能保证企业和外部客户之间会话的保密性
- PPTP：让远程用户拨号连接到本地ISP、通过Internet安全远程访问公司网络资源；有两种不同的工作模式，被动模式和主动模式

- L2F：可以在多种介质上建立多协议的安全虚拟专用网，它将链路层的协议封装起来传送
- L2TP：在PPTP和L2F的基础上产生，适合组件远程接入方式的VPN

12.2.2 第三层（网络层）隧道协议

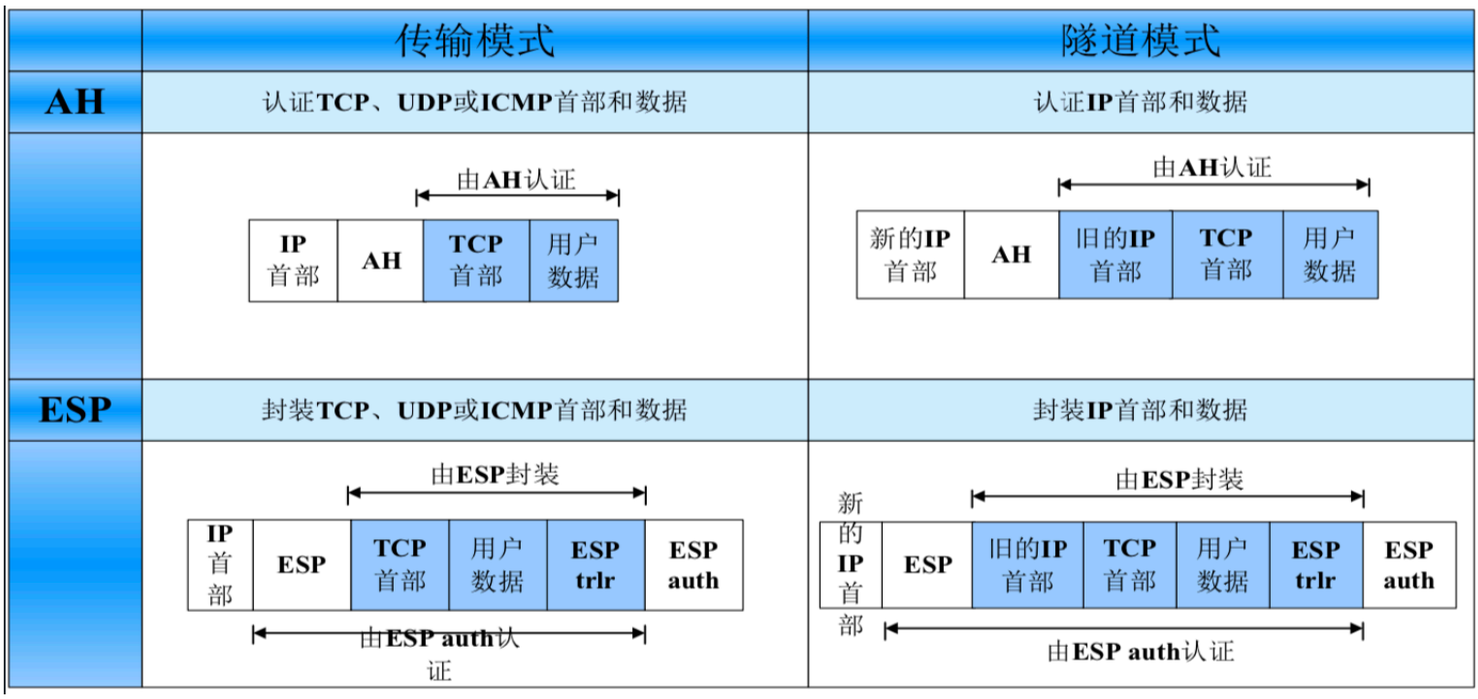
- IPSec：专为IP设计提供安全服务的一种协议
- 通用路由封装 GRE（Generic Routing Encapsulation）：规定了如何用一种网络协议去封装另一种网络协议的方法
- MPLS：引入了基于标记的机制；它把选路和转发分开，用标签来规定一个分组通过网络的路径

12.3 IPSec VPN的原理

在IPv6的制定过程中产生，提供IP层的安全性

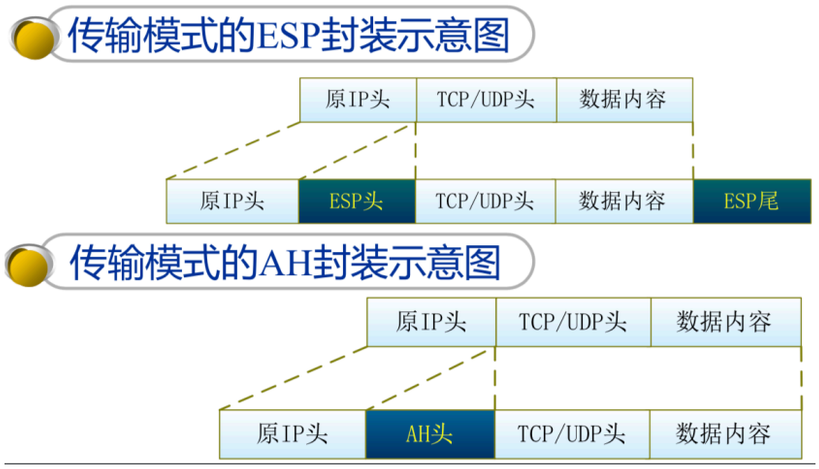
12.3.1 IPSec 协议概述

- IPSec 协议使用 认证头标AH 和 封装安全净载ESP 两种安全协议来提供安全通信。两种安全通信都分为 隧道模式 和 传输模式
- 传输模式用在 主机到主机 的通信，隧道模式用在任何 其他方式 的通信

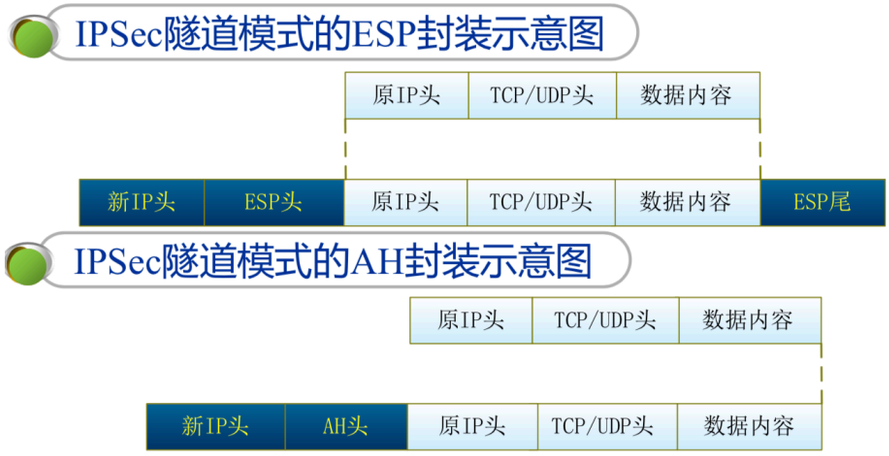


12.3.2 IPSec 工作原理

传输模式：IPSec只对**IP数据包的净荷**（除去IP头的数据）进行加密或认证；封装数据包继续使用**原IP头部**；IPSec协议新产生的头部插入到**原IP头部和传输层协议头部**之间



隧道模式：IPSec对**整个IP数据包**进行加密或认证；产生一个新的IP头，IPSec头被放在**新IP头和原IP数据包**之间



12.3.3 IPSec 中的主要协议

IPSec 主要由 AH、ESP、IKE 来实现加密、认证和管理交换功能

1. AH：认证
2. ESP：加密
3. IKE：动态建立**安全关联**（SA，Security Association）。这个协议有两个阶段：
   - 第一阶段：建立IKE安全关联，即在通信双方之间协商密钥
   - 第二阶段：利用这个既定的安全关联为IPSec建立安全通道

12.3.4 安全关联

当两个网络节点在IPSec的保护下通信时，它们必须协商一个SA（认证）或两个SA（认证+加密），SA有传输模式和隧道模式两种

12.4 TLS VPN的原理（这部分不考，但是我多整理了）

- SSL VPN也称作传输层安全协议（TLS） VPN
- TLS 协议主要用于 HTTPS 协议中
- 优点：用户不需要安装和配置客户端软件
- TLS 协议属于第三层协议

12.4.1 TLS VPN原理

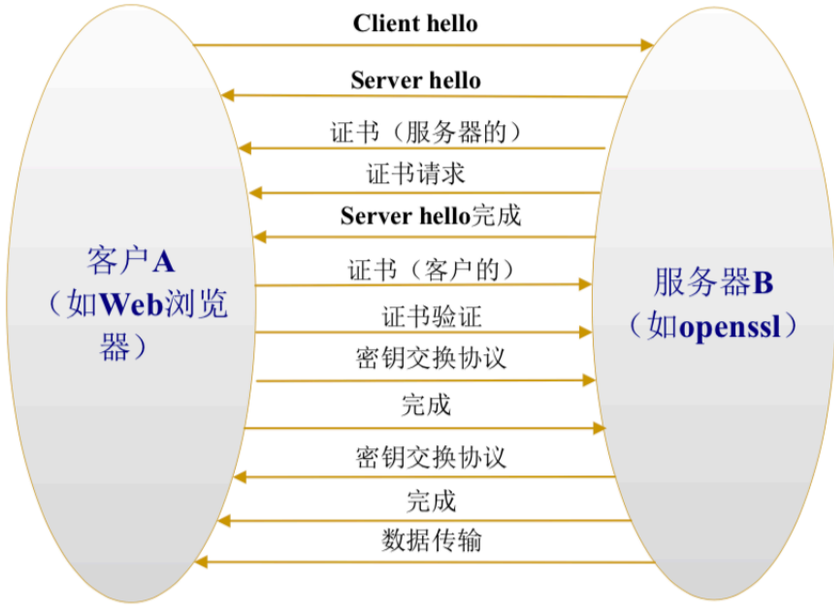
在企业的防火墙后面放置一个**TLS代理服务器**

过程：假如用户想安全地连接到公司网络，

- 首先要在浏览器上输入一个URL
- 该连接请求将被TLS代理服务器取得
- 用户通过身份验证
- TLS代理服务器提供用户与各种不同应用服务器之间的连接

TLS VPN的实现主要依靠下面三种协议支持：

1. 握手协议。具体协议流程：
    - TLS客户机连接至TLS服务器，并要求服务器验证客户机的身份
    - TLS服务器通过发送它的数字证书 证明其身份
    - 服务器发出一个请求，要对 客户端的证书 进行验证
    - 协商用于消息加密的 加密算法 和用于完整性检验的 Hash函数
    - 客户机随机生成一个随机数，用 服务器的公钥 对其加密后发送给TLS服务器
    - TLS服务器通过发送 另一个随机数 做出相应
    - 对以上两个随机数进行Hash运算，从而生成会话密钥



2. **TLS记录协议**：建立在TCP/IP协议上，用在实际数据传输开始前通信双方进行身份认证、协商加密算法和交换加密密钥等
3. **警告协议**：提示何时TLS协议发生了错误