防火墙原理

Presented by:

sunyanghua

某某公司 信息部

目录

1、网络风险与常见攻击

- 网络复杂的结构和用户
- 业务需求需开放服务
- 主机系统服务漏洞
- TCP/IP协议的开放弱点
- 各类攻击工具易获得
- 安全教育不足

1、网络风险与常见攻击

Table 3. Top attacked ports by percentage of attackers

Rank	Port	Description	Percentage of Attackers
1	TCP/135	Microsoft/DCE-Remote Procedure Call (Blaster)	32.9%
2	TCP/80	HTTP/Web	19.7%
3	TCP/4662	E-donkey/Peer-to-peer file sharing	9.8%
4	TCP/6346	Gnutella/Peer-to-peer file sharing	8.9%
5	TCP/445	Microsoft CIFS Filesharing	6.9%
6	UDP/53	DNS	5.9%
7	UDP/137	Microsoft CIFS Filesharing	4.7%
8	UDP/41170	Blubster/Peer-to-peer Filesharing	3.2%
9	TCP/7122	Unknown	2.5%
10	UDP/1434	Microsoft SQL Server (Slammer)	2.4%

Source: Symantec Corporation
TMSdata

1、网络风险与常见攻击

- 一个典型的攻击者工具包

网络扫描器
口令破解
报文监听
特洛伊木马程序
修改系统日志的工具
隐藏活动的工具
自动修改系统配置文件的工具

1、网络风险与常见攻击

- 常见攻击

1、拒绝服务攻击（ Denial of Service -DOS）

- ▶死亡之ping（>64KB的ICMP包，导致TCP/IP协议栈崩溃，接收方死机）
- ▶泪滴teardrop（伪造IP碎片内容，导致TCP/IP协议栈崩溃）
- ▶UPD洪水（产生大量无用数据流，恶意占用带宽和主机处理能力）
- ▶SYN洪水（利用TCP的ACK机制，使主机拒绝有效连接请求）
- ▶LAND攻击（伪造源地址和目的地址相同的SYN包，主机接收大量空连接）
- ▶Smurf攻击（修改ICMP应答地址为受害网络地址，大量广播包阻塞网络）
- ▶畸形消息攻击（修改应用层数据包，造成操作系统服务崩溃）

2、利用型攻击

- ▶口令猜测
- ▶特洛伊木马
- ▶缓冲区溢出

1、网络风险与常见攻击

- 常见攻击

3、信息收集型攻击

►扫描技术（地址扫描、端口扫描）

►操作系统探测（利用NT与Unix的TCP/IP堆栈实现不同，获取主机操作系统）

►网络服务探测（利用DNS和LDAP协议认证缺陷，获取网络和用户信息）

4、假消息攻击

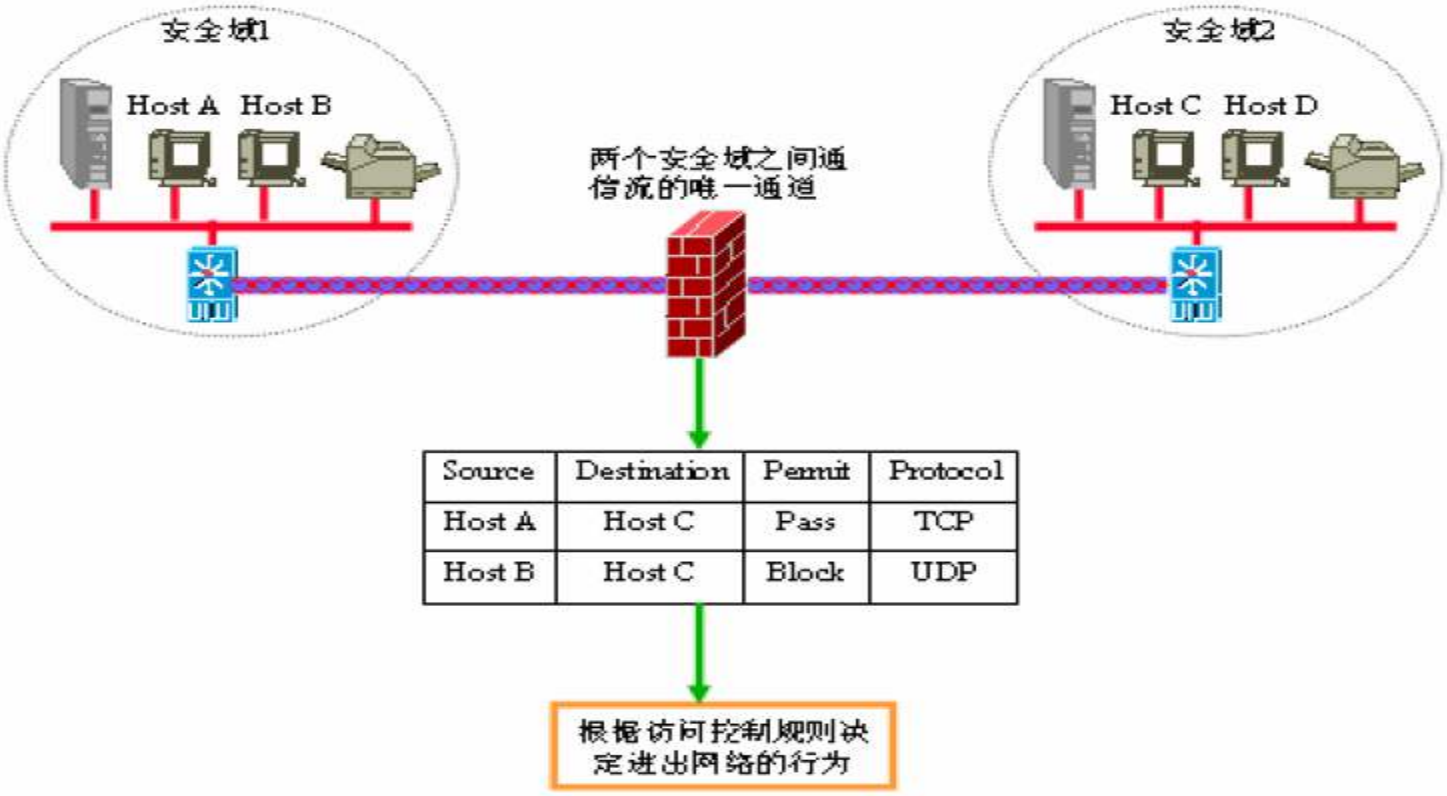
►DNS缓存污染（DNS交换不认证身份，修改DNS信息，使主机发往错误地址）

►伪造电子邮件（SMTP不对发送者身份确认，伪造邮件，附加木马程序）

1、网络风险与常见攻击

如何解决：

正确应用防火墙为核心的网络边界安全设施



2、防火墙基础

- 防火墙定义

百度百科：

是一项协助确保信息安全的设备，会依照特定的规则，允许或限制传输的数据通过。防火墙可以是一台专属的硬件也可是架设在一般硬件上的一套软件。

Rich Kosinski (Internet Security公司总裁）

防火墙是一种访问控制技术，在某个机构的网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问。换句话说，防火墙是一道门槛，控制进/出两个方向的通信。

2、防火墙基础

- 防火墙发展历程

1986年Digital推出第一台商用防火墙。

第一代：包过滤路由器。

如ACL。审计功能弱，过滤规则复杂，降低路由性能。

第二代：代理服务器。

应用级。每一网络应用设计一代理，纯软件，延迟大，安全性低。

第三代：基于通用OS 。

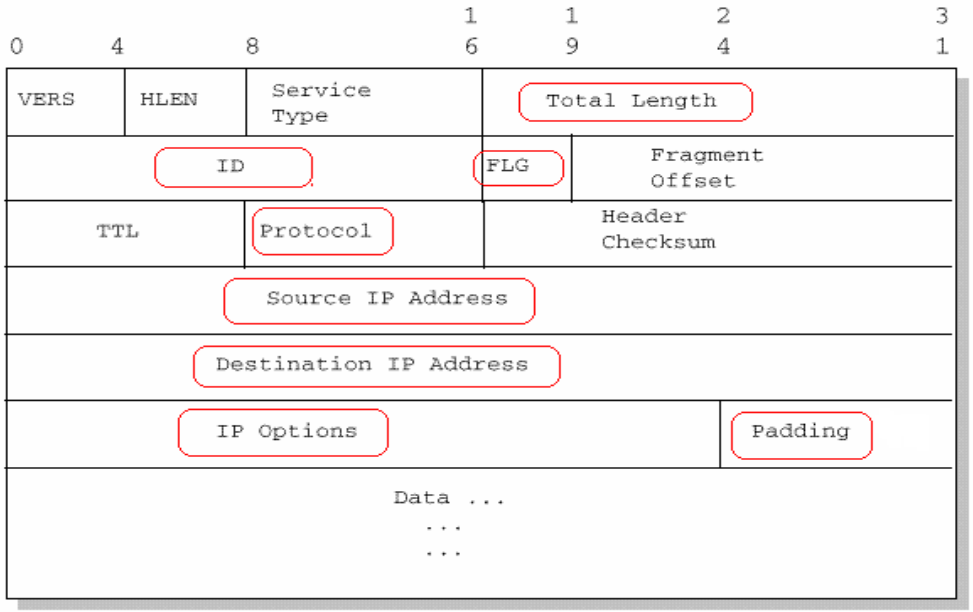
OS自身的安全性能导致防火墙安全能力不足。

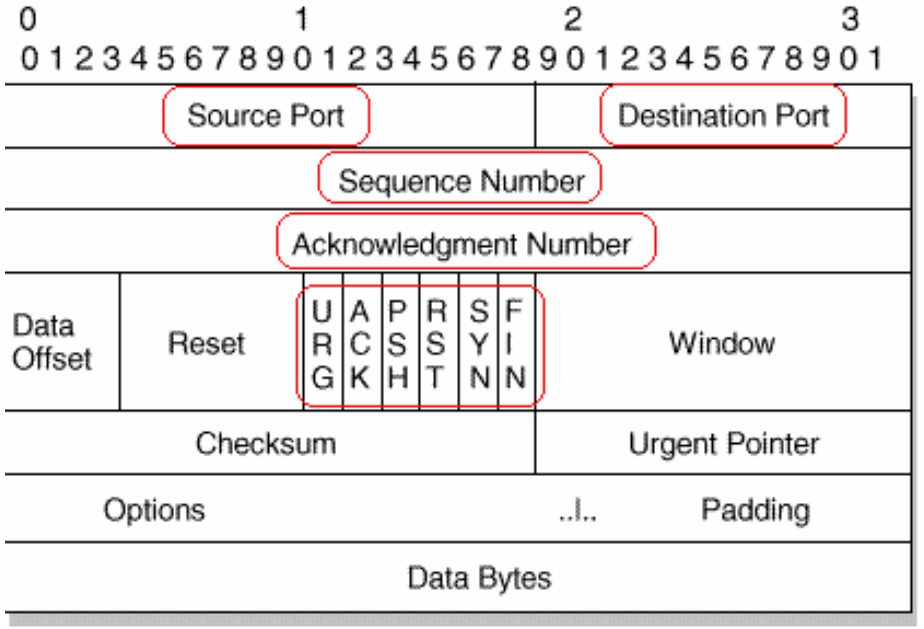
第四代：专用硬件和安全OS 。

专用防火墙OS，增强系统自身安全性；高处理能力，集成多功能。

2、防火墙基础

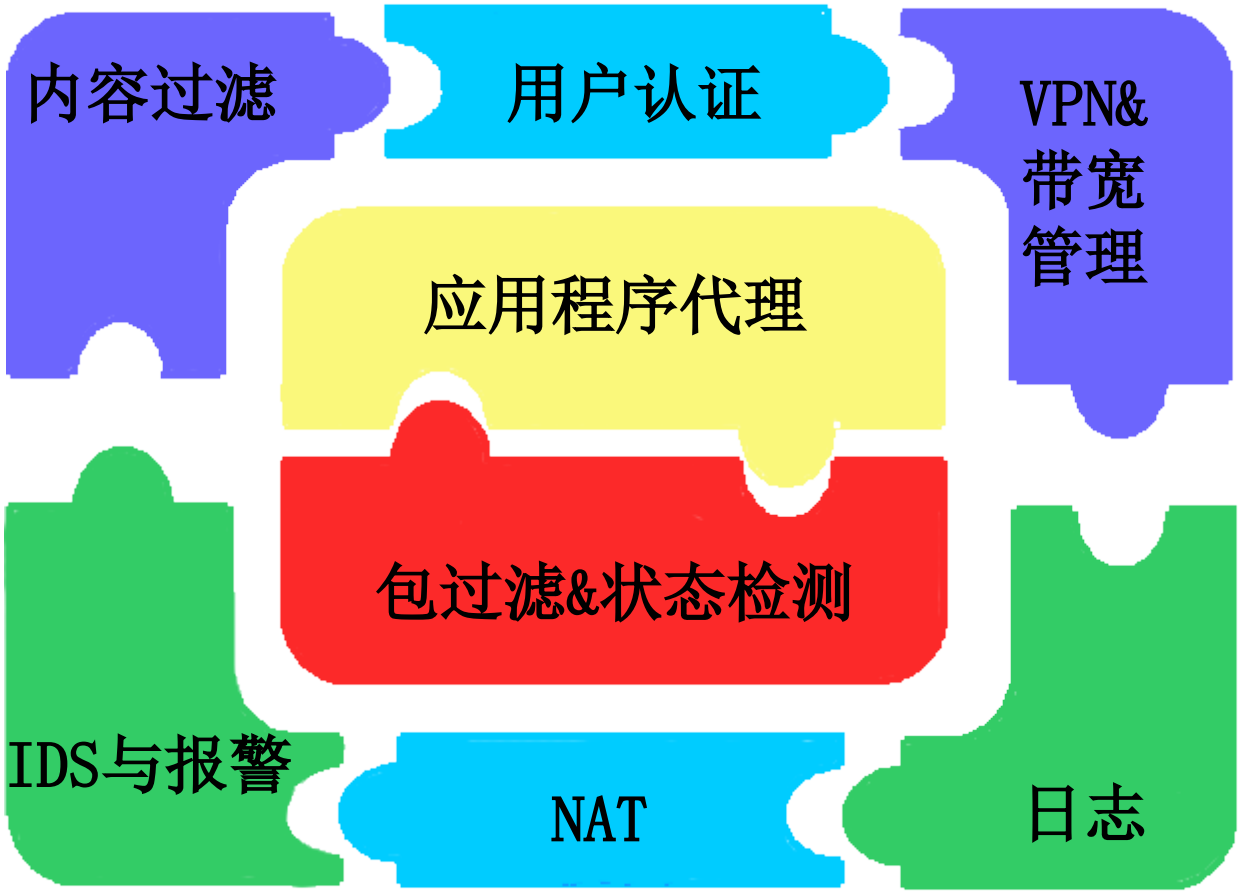
- IP报头&TCP报头





2、防火墙基础

- 防火墙的基本功能



2、防火墙基础

- 防火墙种类—包过滤防火墙

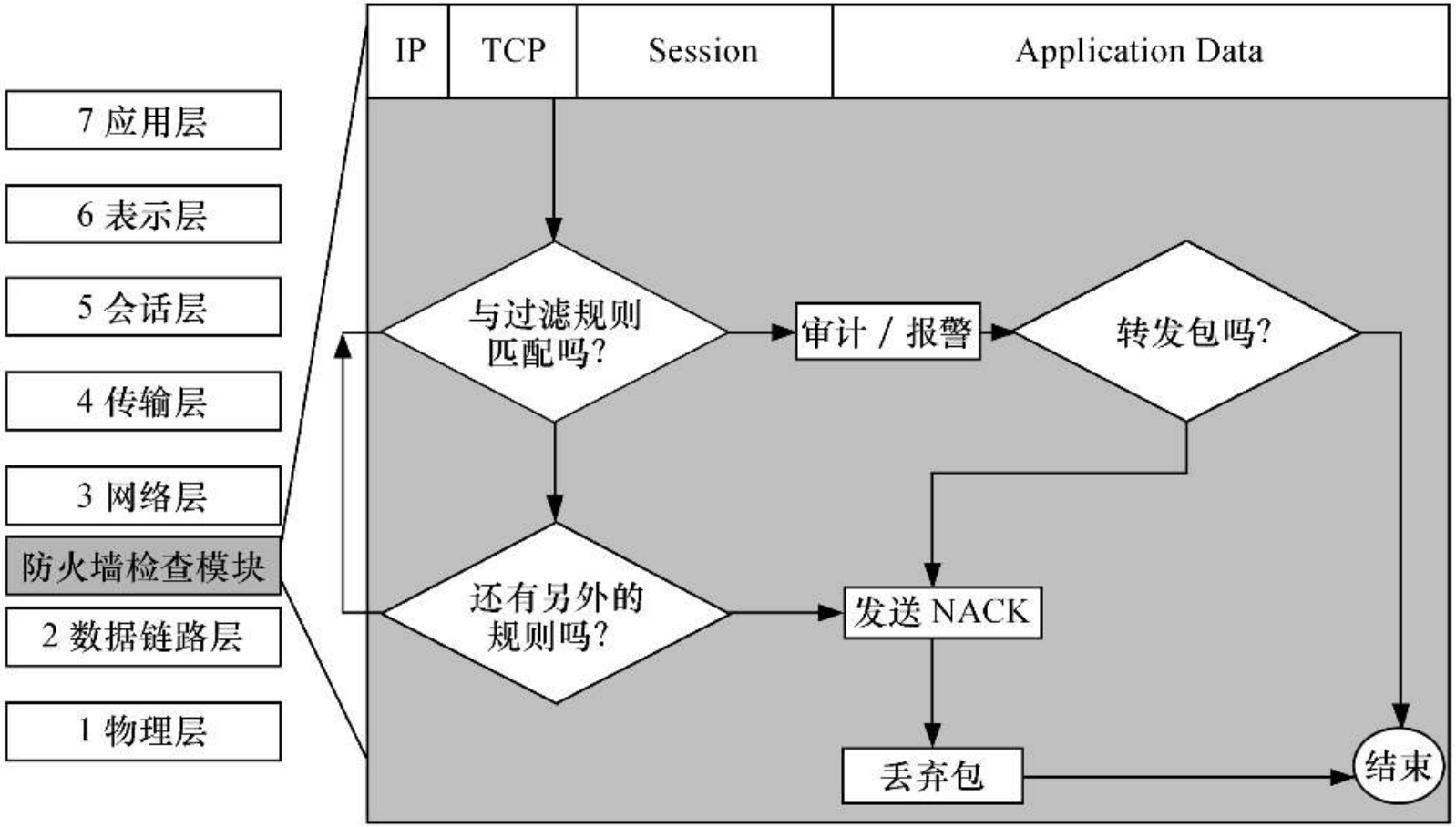
包过滤防火墙对所接收的每个数据包做允许/拒绝的决定。防火墙审查每个数据包以便确定其是否与某一条包过滤规则匹配。过滤规则基于可以提供给IP转发过程的包头信息，包头信息中包括IP源地址、IP目标地址、协议类型（TCP包、UDP包和ICMP包）、TCP或UDP包的目的端口、TCP或UDP包的源端口、ICMP消息类型、TCP包头的ACK位、TCP包的序列号、IP校验和等。

如：HTTP（80）FTP（21）

SMTP （25） Telnet （23） ……

2、防火墙基础

- 防火墙种类—包过滤防火墙



2、防火墙基础

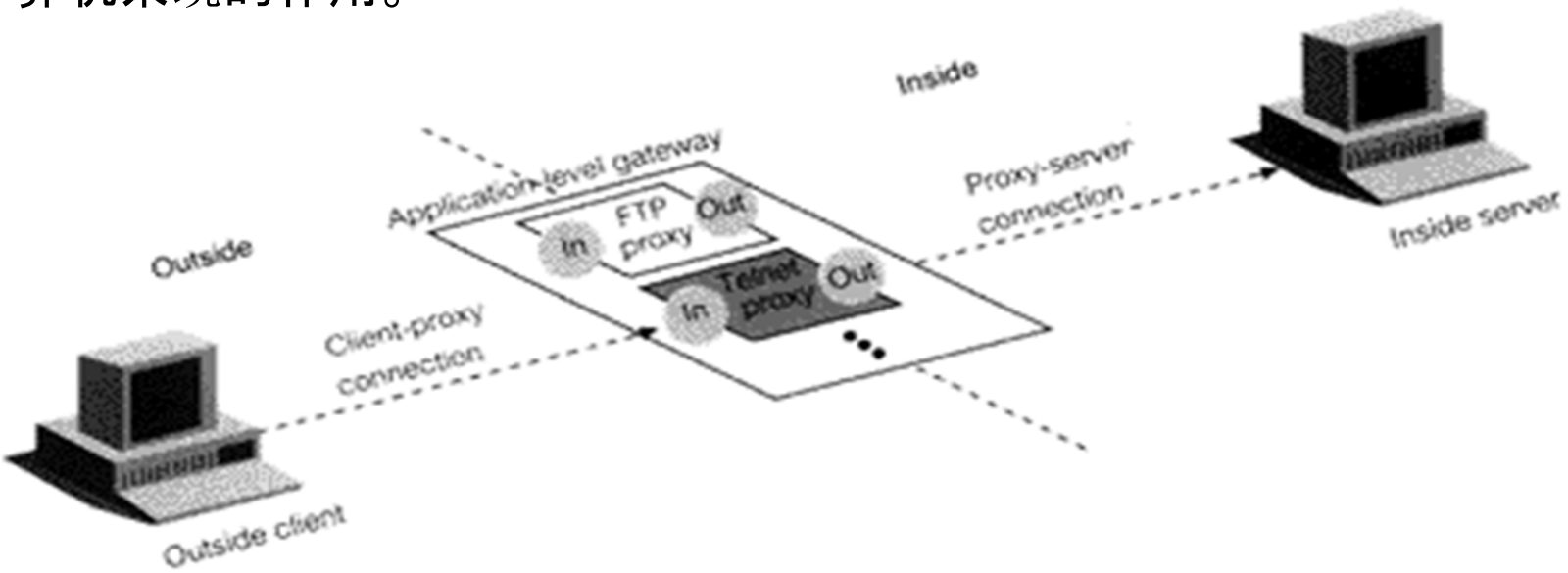
- 防火墙种类—包过滤防火墙

优点：
· 速度快，性能高
· 对用户透明

缺点：
· 维护比较困难(需要对TCP/IP了解　限制策略or宽松策略)
· 安全性低(IP欺骗、小碎片攻击等)
· 不了解主机间会话关系
· 不能根据状态信息进行控制
· 不能处理网络层以上的信息
· 无法对网络上流动的信息提供全面的控制
· 规则配置存在安全隐患，易存在失误

2、防火墙基础

- 防火墙种类—代理防火墙
  - 代理服务是运行在防火墙主机上的专门的应用程序或者服务器程序。不允许通信直接经过外部网和内部网。
  - 将所有跨越防火墙的网络通信链路分为两段。
  - 防火墙内外计算机系统间应用层的“链接”，由两个终端代理服务器上的“链接”来实现。
  - 外部计算机的网络链路只能到达代理服务器，从而起到了隔离内外计算机系统的作用。



2、防火墙基础

- 防火墙种类—代理防火墙

代理防火墙最突出的特点是，将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个代理服务器上的“链接”来实现，外部计算机的网络链路只能到达代理服务器，从而起到隔离防火墙内外计算机系统的作用。此外，代理防火墙在发现被攻击的迹象时，将向网络管理员发出警报，并保留攻击现场。也就是说，在代理服务中，内部各站点之间的连接被切断了，代理服务在幕后操纵着各站点间的连接。